DEPARTMENT OF INFORMATION TECHNOLOGY

STATE OF CALIFORNIA

1997 ANNUAL REPORT

Pete Wilson
Governor

John Thomas Flynn
Chief Information Officer

Table of Contents

Executive Summary

The Department of Information Technology (DOIT) has made substantial progress during the first 24 months of its existence.

In 1997, the DOIT built upon the foundation that both Governor Wilson and the Legislature envisioned when Senate Bill 1 (Chapter 508, Statutes of 1995) by Senator Alquist was signed by Governor Wilson in October 1995.

The DOIT will make 1998 an equally productive year, as many of the projects initiated during 1997 will be in full utilization in 1998.

A number of goals and projects have been accomplished by the DOIT

They include:

- IT Strategic Plan for State of California Developed
- Enterprise Systems Strategy Put In Place
- Data Center Consolidation Study Completed
- Privatization of the State's Telecommunication Networks Initiated
- Reducing the Risk of State Computer Projects
- Training State Information Technology Project Managers
- Providing leadership with the Year 2000 Conversion Challenge

Statewide Plan for Information Technology

Developing a statewide plan for information technology was a keynote of the DOIT's work during 1997. The DOIT developed a *State of California IT Strategic Plan* with input from the Information Technology Coordinating Council (ITCC) and California Information Technology Committee (CITC). The plan provides a vision into the next century, sets strategic directions that allow this vision to be realized, and – most importantly – describes the necessary steps which must be taken. By putting aside a "business-as-usual" mentality, the strategic plan provides an enterprise-level view of the state's information technology (IT) resource as it exists today, and what it should be tomorrow.

Five key strategies have emerged from this plan:

- ❖ IT policy reform encompassing procurement;
- ❖ Infrastructure re-engineering encompassing network consolidation;
- ❖ Statewide IT initiatives encompassing the Year 2000 program;
- ❖ Strategic initiatives encompassing electronic commerce; and
- ❖ Emerging issues encompassing staff recruitment and retainment, and information privacy and security.

For each strategy, action steps are specifically outlined in the strategic plan, setting the agenda for the next two to three years as California moves toward establishing a consistent and comprehensive statewide vision of what IT will be in the 21st century. This strategic plan provides not only the guiding vision, but also the common direction for all state entities to use as individual agency and departmental IT strategic plans are developed.

Reducing Project Risk

The challenges associated with implementing state information technology projects remain very real. In fact, risk will always be high for complex projects. Moreover, this risk is inherent in information technology projects, and is by no means unique in California state government.

Research indicates that more than 31 percent of the approximately 175,000 information technology development projects in the United States will be canceled prior to completion. The research also indicated that 52 percent of the projects nationwide will cost nearly twice as much as their original budgets, while only 16.2 percent of projects will be completed on-time and on-budget. In large companies – California state government falls into this category – only 9 percent of projects will be completed on-time and on-budget. In 1995, American companies and governments spent a combined $81 billion on canceled software projects.

Those statistics demonstrate that the risk of information technology project failure is an uncomfortable reality in all sectors – public and private. Therefore, some failure can be anticipated.

What does this mean for California? Some software projects are bound to fail for one reason or another. The key is to identify areas where the state can increase the odds for success – thereby reducing the likelihood of failure.

The goal of the DOIT's oversight effort is to minimize the potential for failure through a combination of methods so that over time California achieves an increasingly higher ratio of project success. Accordingly, the DOIT has focused on the following primary tools for mitigating risk:

- Reform of the project initiation and approval process;
- Utilization of private, independent consultants for project management and oversight;
- Creation and required use of the DOIT's Risk Assessment Model (RAM);
- Reform of the procurement and contract processes;
- Implementation of enhanced project tracking information; and
- Use of risk mitigation planning.

In addition, the DOIT has already set the foundation to improve risk mitigation by:

- Improving and providing additional protections in the state's model contract for IT projects;
- Requiring new system development projects to utilize alternative procurement and project management methodologies;
- Requiring the use of external experts to assist state IT projects in the areas of project management, oversight contract management, and contract drafting and negotiation; and
- Establishing a peer-review process to subject major projects to periodic reviews by a panel of experts, which may include a mix of state and private sector individuals.

Enterprise Systems

Each fiscal year the State of California spends nearly $2 billion on information technology and telecommunication systems. Many of these systems produce, use and process management information that has value to multiple state agencies. However, because the state has traditionally delegated a great deal of administrative responsibility to individual departments, no strategic policy has existed to ensure that these expenditures provide the greatest possible benefit to state business operations at the least possible cost.

In response, California's Chief Information Officer commissioned the Enterprise Systems Subcommittee of the state's Information Technology Coordinating Council (ITCC) to develop a statewide strategy for developing and implementing systems that are enterprise-wide in scope.

In September 1997, the Enterprise Systems Subcommittee completed its final report, the highlights of which include:

- Establishing several pilot enterprise systems designed and implemented to allow evaluation of alternative approaches to state enterprise systems;
- Setting a moratorium on development of enterprise systems until selected pilots have been implemented, evaluated and determined to be effective models; and
- Developing a uniform, statewide vendor policy to reduce unnecessary costs and redundant purchases.

The DOIT has already begun discussions with representative agencies and departments within state government to sharpen focus on candidate pilot enterprise systems.

Restructuring the State's Data Centers

In compliance with the requirement of SB 1, the DOIT completed and delivered by the statutory deadline of July 1, 1997, the data center consolidation study entitled *Analysis, Conclusions, and Recommendations on the State of California's Department of Information Technology Data Center Consolidation Study.*

The study, prepared for the DOIT by the Deliotte & Touche Consulting Group, spelled out key findings and identified consolidation opportunities that could result in significant saving for the state.

Specifically, the study recommended consolidating the data centers located at the Franchise Tax Board, State Controller's Office, Public Employees Retirement System, California State Lottery, and State Treasurer's Office into the Teale Data Center (Teale), one of the state's existing central data centers. Upon full review of all these issues, the DOIT will consider the next appropriate steps to obtain greater efficiency.

The study recommends considering consolidation of the state's Teale and the Health and Welfare Data Center (HWDC) only after all Year 2000 operational recovery, preparation and testing, business function support, and technical disruption issues have been addressed. Consolidating Teale and HWDC could create significant savings over 10 years, according to the Deloitte & Touche study.

Even before any of its recommendations have been implemented, the Deloitte & Touche study is yielding benefits for the taxpayers. By thoroughly examining Teale's rates and operations, the study was able to identify areas in which the data center will be able to reduce the rates it charges to other state agencies – bringing down the overall cost of government.

The DOIT has drafted, and has enforced in new information technology projects, several of the policies recommended in the study, including the centralization of new systems, enhanced operational recovery provisions, and the consolidation of data center planning and technical efforts. Some of the proposed consolidation activities outlined in the report will be deferred until the next century to allow the completion of the state's Year 2000 compliance efforts in their current locations.

Privatizing the State's Telecommunication Networks

In December 1996, the DOIT partnered with the Department of General Services (DGS) Telecommunications Division to release a new strategic plan for the state's networks. This report, entitled *California Integrated Information Network: A Strategic Plan for CALNET and All State Telecommunications Networks*, made a series of findings regarding California Network (CALNET) and the state's other telecommunication networks, and outlined a strategy to address the problems with CALNET while establishing a process to achieve real network consolidation.

The primary goal of that plan — the privatization of CALNET and the associated network services — has already begun. The DGS, in cooperation with the DOIT, initiated a solicitation for business plans by private telecommunications companies to assume maintenance and operation of CALNET. According to current plans, by early 1998 the state's 225,000 telephone dial tones will be maintained by a private vendor. The selected vendor will provide local switching, long distance services, voice mail and data-transmission services. This project, estimated at more than $500 million over five years, will represent the largest state outsourcing in the nation and is, through increased competition, intended to achieve significant cost savings, provide access to new services and technology, and improve customer service.

Through the DOIT's leadership, the process is well underway to coordinate state telecommunications into a single business entity. The goal is to obtain highly competitive pricing and an unprecedented quality of service to the State of California, which is California's single largest telecommunications customer.

Enhancing Information Technology Security

As the State of California's increasing reliance on information technology grows, issues such as security of vital information become increasingly critical. In response, the DOIT has contracted with the federal Department of Energy's Lawrence Livermore Laboratories Security Incident Technology Center (SITC). This center is a leading nationwide resource for assisting large data information users, such as the State of California, in responding to potential or actual attacks on large databases by hackers or others with mischievous or criminal intent.

Since November 1997, the SITC has provided an incident reporting and response capability for the state to use. This system now provides a secure, encrypted system to allow state agencies and departments to file online reports of security incidents. The SITC then gathers this information and provides monthly summaries of these incidents to individual state departments and agencies, including actual experienced attack methods, emerging threats, preventative measures and which databases appear to be the most frequently targeted. This information is being shared with the DOIT so that existing policies can be modified to address changing attack and prevention technologies. Emergency bulletins will be utilized, when needed, to advise when a new attack method surfaces.

The DOIT clearly understands the government's custodial responsibility for confidential and sensitive information about citizens, businesses and organizations. This precedent-setting alliance with Lawrence Livermore Laboratories, which has national implications, is one of several steps the DOIT is taking to ensure that the state's information technology systems are planned, constructed and maintained in a responsible manner to maintain public trust and confidence.

The Pursuit of Excellence: Investing in State Projects and Managers

Project management in California government can represent a major category of risk, or serve as a valued asset. This dichotomy is a direct result of the diffused approach state government has taken with respect to information technology projects. The DOIT has determined that in some cases the lack of appropriate project management continues to be a significant barrier toward the implementation of successful state projects. Some departments are better able than others to manage their information technology projects. However, even the most experienced department may find its project management capabilities inadequate for a particularly challenging project.

To address this disparity and create a benchmark for project management expertise, the DOIT has established an official program to train and certify project managers in cooperation with the University of California at Davis. This is the first executive government/higher education partnership in the nation to certify state managers for IT project management.

Because this training program is new and the need for project managers whose qualifications meet the levels of risk and complexity of existing, ongoing projects is immediate, the DOIT has moved aggressively to ensure capable managers are available. The DOIT has mandated as a condition of project approval that project management be acquired from an external source if insufficient expertise exists within a department. In addition, this requirement may be imposed on currently-approved or ongoing projects in instances where complications and/or difficulties arise which can be directly attributed to poor or inadequate project management.

Addressing the Year 2000 Challenge

This past year has been both challenging and rewarding for the DOIT's California 2000 Project Office. However, much work remains to be accomplished – not just by the California 2000 Project Office, but by all IT officials at all levels of state government if this fundamental challenge to the state's large databases and systems is to be met. It is, in fact, the largest comprehensive IT project in the state's history.

The Year 2000 represents a threat to computer systems throughout the world. The problem arises because most computer programs created during the last 30 years assume that all dates fall within the 20th century. Unless corrective action is taken, business functions that depend on correct understanding and manipulation of dates will begin to fail as the turn of the century approaches.

The DOIT has worked toward enhancing awareness at all levels of state government through presentations to the Governor's Office, the Governor's Cabinet, the Legislature and the staff and directors of all state agencies and departments.

On a parallel track, the California 2000 Project Office has collected information on existing computer applications from across the State of California. The office has distilled this information for potential impact and determined that more than 1,200 computer systems – 600 of them mission critical – require some form of remediation to become Year 2000 compliant.

Conservative cost estimates to fix these problems now approximate $187 million. More than 300 million lines of computer code will have to be examined, fixed and then tested to ensure that computers can continue working from this century into the next.

Recognizing the urgency of this task, Governor Wilson signed Executive Order W-163-97 in October 1997, declaring that Year 2000 solutions are a state priority, and directing the DOIT to coordinate all Year 2000 activities. Specifically, the Executive Order calls for:

- Limiting new computer projects to those mandated by law;
- Requiring each state agency to take responsibility to find and fix Year 2000 problems by December 31, 1998;
- Protecting essential computer systems from corruption by other systems that are not Year 2000 compliant; and
- Requiring any new purchases of systems, hardware, software or equipment to be Year 2000 compliant.

Governor Wilson's executive sponsorship gives the state's information technology professionals the commitment they need to follow this mission critical task to completion. The DOIT takes its responsibility for oversight of this project seriously. In response, Governor Wilson gave the DOIT clear performance guidelines. Specifically, the Executive Order requires the DOIT to:

- Define Year 2000 compliance standards for the state;
- Require quarterly update reports from each state agency;
- Provide Year 2000 progress reports quarterly to the Administration and the Legislature;
- Foster solutions to the problems presented by embedded microchips in automated devices; and
- Address Year 2000 legal issues which may directly or indirectly affect state services.

The December 31, 1998, deadline was established to give all state agencies time to test and ensure that computer applications will work correctly to process the day-to-day workload the systems were designed to handle. Some systems throughout the state that need correction to handle the Year 2000 date will remain uncorrected by December 31, 1998. However, the DOIT believes that with the detailed action plan, the mission critical systems with the most impact on the lives of citizens and taxpayers of California will be successfully remediated and deployed.

New Trends and Technologies: The DOIT's Vision for California's Future

Few technologies offer as much potential benefit to government and citizens as those associated with the Internet and the World Wide Web. The easy use and low cost of these tools have led to their widespread adoption by businesses, organizations, governments and citizens. The Internet is becoming a universal computer network, used by nearly all businesses and a growing proportion of private citizens, and presenting a completely new means for government to deliver its services and perform its functions.

California state government has kept pace with this development, with nearly all state agencies offering web pages. Most of the web pages provide substantial information on the functions of their sponsoring agencies and provide means of contacting the agencies for assistance or services. By July 1998, all such web pages will be required by statute to include a complaint form that can either be completed and submitted online or printed and mailed conventionally. The California State Library has sponsored a particularly high-quality page which serves as an index and gateway to the individual Internet presentations of the other state agencies. This web page is recognized for its comprehensive and convenient format.

Despite the ease of use these pages represent, they do not offer all the kinds of interaction that citizens perform with government services. The majority of government contact with the public, businesses, organizations and other governments involves either specific information requests or the need to conduct a transaction of some sort. By using electronic government technologies to replace the current methods of doing these kinds of activities, the state can achieve much greater reductions in cost and effort to the state and its clients.

To be sure, there are often significant barriers to these efforts. There has been considerable discussion of the issues of transmission security and the public fear that transactions they make over the Internet will be intercepted. The structure of the Internet provides more opportunities for eavesdropping than do telephone networks, but it is fairly easy to encrypt the transmission of sensitive information such as credit card numbers to effectively prevent this.

Considerable industry effort is being devoted towards the problem of authentication, and potential technical solutions have been identified. Perhaps most promising is the technology involving digital signatures and certification. An individual is assigned a unique digital message, or certificate, that can be transmitted over the Internet to identify the individual to a potential business partner, including the government. This identifier is provided by a third party, known as a certification authority, who initially verifies the person's identity using conventional means, and countersigns that certificate. The government or business does not need to recognize each individual, but needs only to know and trust the certifier's countersignature.

This methodology provides additional benefits. An individual's certificate includes a unique key, which the government agency or business can use to encode its communications with the individual so that only that individual can read the message, thus preventing problems with eavesdropping or misdelivery. Because only the owner of the certificate knows that key, it can be presumed that only that person can have participated in a conversation using that identifier. This achieves a more difficult task: preventing a person from denying that he sent, or received, a particular communication. Known as non-repudiation, this capability is essential for activities, such as tax filings, where the communication, and its accuracy, are enforced by law.

Related to both the problem of secure transmission and authentication is the issue of electronic payment. In the current environment, it is fairly difficult to exchange credit information over the Internet in a safe manner. Over the long term, the DOIT anticipates that credit cards and authenticating smart cards are likely to be combined into a single consumer product, so that one is at once authenticated as an individual and as a credit bearer. The DOIT therefore cautions against state efforts to distribute authentication certificates for large portions of the public, as that effort is likely to be superseded by such credit/identity certificates.

The DOIT believes that authentication and other electronic means to communicate and conduct typical business transactions, while only

in their infancy today, will develop as rapidly as the use of the internet has. The DOIT believes that electronic commerce represents an historic change in the fundamental relationship between government and the public. Careful and considered implementation of these technologies, with sensible plans and real partnerships with industry, will achieve better, faster, cheaper, and most importantly, friendlier government.

Project Initiation and Approval

The DOIT has been given responsibility throughout the project lifecycle for enforcing practices to increase the likelihood of project success. In addition, the DOIT is required to add an enterprise perspective to planning, implementing and operating state IT projects. These goals require the DOIT to perform tasks in support of project initiation which are substantially different than those performed in the past. Consequently, substantial policy reform focused in the areas of project initiation and approval is required.

The DOIT, in cooperation with the Department of Finance (DOF), defined a new methodology governing the consideration of approval and funding of IT-related proposals, as published in a report to the Joint Legislative Budget Committee in December 1997, entitled *State of California Information Technology Project Initiation and Approval Report*.

The purpose of the new methodology is to: (1) establish a uniform format for use by state departments and agencies in identifying and reporting their respective IT project needs and statuses, and (2) enhance the coordination between the DOIT and the DOF regarding the consideration of requests for funding IT projects.

Department History and Organization

History

Two years ago, the Department of Information Technology (DOIT) was created pursuant to the provisions of Senate Bill 1 (Chapter 508, Statutes of 1995), which Governor Wilson signed into law in October of 1995. This new department was challenged to bring statewide coordination to California state government's information technology (IT) and telecommunications systems and to ensure that the state receives maximum benefit from its nearly $2 billion annual investment in these technologies.

The Department of Information Technology was created on January 1, 1996, and given authority to coordinate the acquisition, use, and management of information and telecommunications technology throughout state government.

After conducting a nationwide search for candidates, Governor Wilson appointed California's first Chief Information Officer in November 1995.

The DOIT has created and appointed members to the California Information Technology Commission (CITC), a group of experts from private industry, academia, and federal and local government, and the Information Technology Coordinating Council (ITCC), a group of information technology and policy executives from within state government.

January 1, 1996, marked not only the beginning of the DOIT, but also the culmination of efforts by many to initiate a fundamental reform of the state's use and management of information technology. In 1994, Governor Wilson created the Task Force on Government Technology Policy and Procurement, which conducted an expedited, 60-day review of state information technology practices. This group of private sector information technology professionals agreed on two fundamental themes:

Investment in Information Technology Will Increase California's Competitiveness. As the economy becomes more information-driven, states in which government and business are able to form strategic partnerships to provide information-based products and services will have a competitive advantage. The task force found that California is in a position to develop such a competitive advantage.

The Concept of Public Trust Must Be Redefined. At the time the task force conducted its review, public perception was that state government was too large and too slow-moving to keep pace with rapidly advancing computer and telecommunications technologies. While it is not possible to assure the public that there will be no more IT project failures, the task force recommended that the state adopt policies that would mitigate the risk associated with projects and ensure that failures are identified sooner.

The task force's report provides a remarkably comprehensive blueprint for reform, considering the short time which it had to perform its work.

The members developed multiple recommendations in four major subject areas: planning and organization, management and accountability, procurement, and personnel. However, the task force itself acknowledged that its report was not intended to be a checklist of action items to be performed. The report stated that "once appointed, the CIO should have full latitude regarding how organizational and policy changes are implemented, although they would likely be based on the CIO's assessment and further investigation of issues." In addition, the task force acknowledged that its review was not comprehensive and that "there is more work to be done in studying the state's information technology policies and practices."

To build on the work of the task force, in July 1994 Governor Wilson assembled some of the brightest minds from California's world-class, private sector high technology industry into the Governor's Council on Information Technology. This group undertook an exhaustive study and issued recommendations urging state agencies to re-examine their core functions. The Council's report, entitled *Getting Results*, is a guiding document for the work being done at the DOIT.

The Legislature has also taken action to reform the state's use and management of information technology. The Legislative Analyst's Office issued a report in June 1994 entitled *Information Technology: An Important Tool for a More Efficient Government*, and another report in January 1996 entitled, *Information Technology: An Update*. These reports made specific recommendations to the Administration to reform information technology. The Legislature's most significant action to date has been the enactment of Senate Bill 1 in 1995, this department's enabling legislation.

Taken together, the reports of the task force and Governor's Council and Senate Bill 1 identify literally hundreds of discrete action items for the DOIT and form a standard by which its work can be measured.

Department Organization

The DOIT has been structured into four divisions and two offices which address the areas of responsibility assigned to the department. The DOIT is staffed in accordance with current budget allocations. Furthermore, in anticipation of the state's accelerating reliance on IT investment and the concomitant increase in the department's duties and responsibilities, the DOIT has proposed commensurate staff augmentation in Fiscal Year (FY) 1998/99.

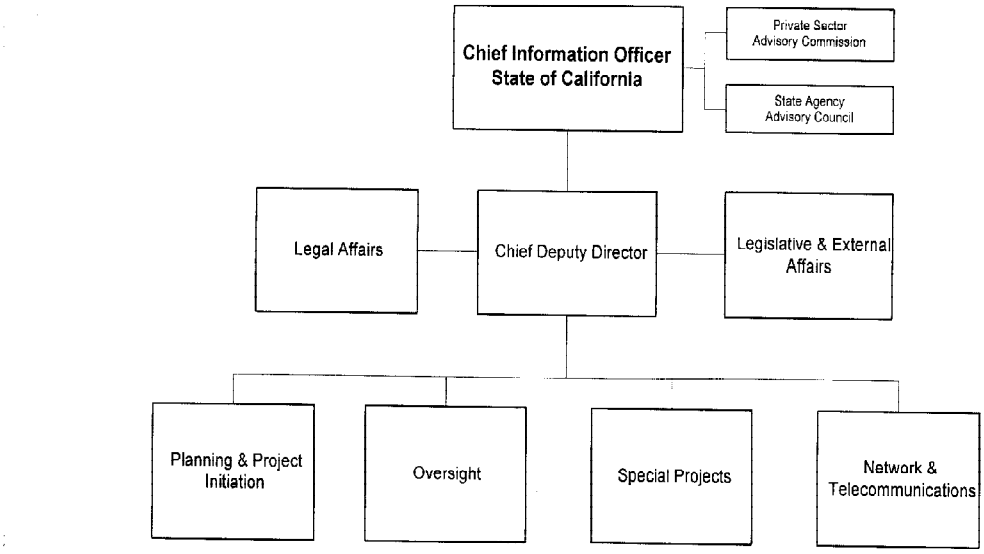
Chief Information Officer

A consistent theme among *Getting Results*, the report of the Task Force on Government Technology Policy and Procurement, and Senate Bill 1 is the need for greater statewide coordination of information technology investment and applications. Specifically, SB 1 gives the DOIT responsibility for the "development of statewide vision, strategies, plans, policies, requirements, standards, and infrastructure."

A key component of this statewide coordination was the creation by Executive Order W-120-95, and subsequently by SB 1, of the position of Chief Information Officer (CIO) for the state reporting directly to the Governor.

SB 1 grants the CIO specific authority to:

- Review proposed information technology projects for consistency with statewide strategies and suspend or disapprove initiation of a project according to that review;
- Make recommendations for remedial measures to be applied to agency information technology projects, including the use of independent oversight;



- ❖ Develop policies and requirements needed to implement SB 1 in the State Administrative Manual (SAM) or by Management Memo.

- ❖ To assist in the day-to-day operations, the State Chief Information Officer established the Legislative and External Affairs Office and the Legal Affairs Office.

Legislative and External Affairs Office

Information technology and telecommunications are issues of significant interest to the Legislature, media and the public. The Legislative and External Affairs Office accommodates requests for information and monitors IT related legislation. This office also serves as liaison to the DOIT advisory committees: the Information Technology Coordinating Council (ITCC) and the California Information Technology Commission (CITC).

Legal Affairs Office

Many IT and telecommunications issues have significant legal ramifications. The rapid development of the information economy is forcing significant changes in major bodies of law that directly impact state government, including copyright, privacy and taxation. The state's telecommunications and IT projects are largely exercises in procurement, which in turn are fundamentally exercises in contract law. The legal counsel ensures that the state's interests are protected and the agencies 'legal staff are provided with the most up-to-date information and resources to effectuate the required legal changes.

Planning and Project Initiation Division

The DOIT created the Planning and Project Initiation Division to assist state agencies and departments in creating IT strategies and plans that will meet their business needs, maximize the return on IT investment and mitigate project risks.

Specifically, the Planning and Project Initiation Division is responsible for:

- ❖ Assisting the CIO in developing California's first statewide information technology strategic plan;

- Providing guidance and assistance to agencies and departments to ensure that their information technology plans are consistent with the statewide information technology strategic plan;

- Reviewing and making recommendations to the CIO regarding approval of Feasibility Study Reports (FSR), Special Project Reports (SPR) and various IT project-related documents.

Oversight Division

Government Code §11700 et. seq. charges the DOIT with responsibility for information technology project oversight. To carry out this responsibility, the DOIT has ensured placement of independent oversight teams on all major projects identified by the department as warranting close attention. Increasing the level of project oversight, both through the efforts of the Oversight Division and through the use of independent private sector experts, continues to be the department's top priority.

Specifically, the Oversight Division is responsible for:

- Providing project oversight on high-risk, large, complex projects;

- Developing statewide project oversight strategies, policies and processes to improve the state's overall management of information technology; and

- Developing and implementing appropriate policies, requirements and processes for risk assessment on information technology projects.

Network and Telecommunications Division

Networks and telecommunications are the foundations which support information technology, enabling computers to be networked and information to be transported and shared. As such, SB 1 gives the DOIT responsibility and authority for state telecommunications policy. The critical nature of this responsibility warranted the creation of the post of Chief Networking Officer, the first position to be so specified by any state in the nation.

The Network and Telecommunications Division has been charged with accomplishing the development and integration of the state's telecommunications infrastructure to meet the needs of California government. This division provides guidance to all state agencies in their use of telecommunications technologies, security and disaster recovery. Major projects for this division include managing the data center and telecommunications network consolidation efforts, and setting state policies relating to messaging, internetworking, operational recovery, and information security.

Special Projects Division

SB 1 charges the DOIT with addressing information technology issues which have statewide implications, thereby avoiding situations where a lack of statewide coordination may result in disjointed, unstructured, incompatible and costly agency-by-agency solutions. The DOIT created the Special Projects Division to identify and address issues of statewide significance such as the Year 2000 and successful implementation of information technology projects. To carry out its responsibilities, this division established two project offices: the CA 2000 Project Office and the IT Project Office.

CA 2000 Project Office

The DOIT's CA 2000 Project Office was created to establish a centralized focal point for statewide coordination of the Year 2000 (Y2K) challenge. The CA 2000 Project Office is administering the CA 2000 Program to ensure the state's mission critical systems become Y2K compliant. It has been successful in planning,

gathering, coordinating, sharing and reporting statewide efforts in meeting the Y2K challenge. The CA 2000 Project Office has the following responsibilities:

- ❖ Develop and maintain a database to facilitate information gathering, sharing and analysis of Y2K activities;
- ❖ Develop tools to assist and monitor entities in their Y2K implementation;
- ❖ Provide guidance and enable assistance in planning and managing Y2K activities;
- ❖ Promote information sharing to leverage inter-departmental resources and achieve economies of scale;
- ❖ Track IT efforts specifically related to Y2K compliance;
- ❖ Report statewide Y2K status;
- ❖ Assess departments 'Y2K funding requests and Budget Change Proposals (BCPs); and
- ❖ Ensure state entities are mitigating the Y2K risk of their mission critical systems and supporting Y2K activities.

DOIT IT Project Office

The DOIT created the IT Project Office to foster a higher success rate for the state's IT projects. The Project Office adheres to a "statewide, enterprise-wide" perspective to ensure that IT projects initiated within state government are consistent with statewide strategies, policies and standards. It advocates successful and effective management of state IT projects through appropriate oversight and advocacy. Additionally, it promotes communication between the Administration and state organizations with regard to business priorities.

Within each state entity, the Project Office promotes a broad-based strategic focus versus individual project focus. The Project Office's goals are as follows:

- ❖ Ensure IT projects are consistent with statewide strategies, policies, standards and state organization business and IT strategies;
- ❖ Promote successful and effective IT project management through oversight and advocacy;
- ❖ Promote partnership between business and IT organizations;
- ❖ Promote organizational focus (versus project focus) and project coordination within state organizations, and assess organizations 'ability to undertake multiple projects;
- ❖ Ensure appropriate monitoring of IT projects to determine when external assessments are required to ensure project success; and
- ❖ Develop and maintain a computer-based system for use by the DOIT, the Legislature and departments for all state information technology projects.

Advisory Councils

Senate Bill 1 (Chapter 508, Statutes of 1995) required the establishment of advisory councils to assist the CIO in developing statewide information technology policy. Accordingly, the DOIT assembled two advisory councils, one consisting of state government information technology and policy executives, the other consisting of experts from the private, academic and nonprofit sectors.

Information Technology Coordinating Council

The internal state advisory committee, the Information Technology Coordinating Council (ITCC), is comprised of senior level policy and technical representatives from the state's agencies. In 1997, members of the ITCC participated on two subcommittees which provided the DOIT with valuable direction and guidance on two major department initiatives. The first subcommittee produced a report in February 1997 which laid the foundation for re-engineering the project initiation and approval process between the DOIT and the Department of Finance. The second subcommittee produced a report in September 1997 to direct the approach that the state uses in development and implementation of state administrative systems. For more information regarding this subcommittee, please see the *Enterprise Systems* section of this report.

California Information Technology Commission

The California Information Technology Commission (CITC) membership represent the private sector, academia, nonprofit organizations and other governmental sectors. California's private technology industry has set the standard worldwide for excellence and innovation. Through the CITC, the DOIT has tapped into the expertise and experience of this invaluable resource, helping to bring proven private sector solutions to state government. The CITC meets on a quarterly basis and subcommittees of the commission meet regularly on a schedule determined by the members. Subcommittees for 1997 included Smart Communities and data center and network consolidation. In December 1997, CITC Chairman John Eger, who also serves as chairman of the California Institute for Smart Communities, produced the draft report, *Towards a Smart California: Community Development Information Technology, State Government, and the Building of Tomorrow's Smart Communities.*

Rosters, meeting agendas, meeting summaries and dates of future meetings are available from the DOIT and are posted on the DOIT web site (www.doit.ca.gov). The meetings of both the ITCC and the CITC are open to the public.

Department Funding

The Governor's Office of Information Technology (OIT), a precursor to the DOIT, was first created by Executive Order W-120-95 on April 13, 1995. That office was funded with a budget of $2.5 million, which came in three equal parts from the General Fund, and reimbursements from the Health and Welfare and Teale Data Centers. Senate Bill 1 became effective January 1, 1996, establishing the DOIT in statute and the 1995/96 budget codified the funding of the new department.

The Legislature adopted language as part of the 1996/97 budget requiring the DOIT and the DOF to develop a funding mechanism to distribute across all state agencies on an equitable basis the DOIT's annual budget. As a result, the DOIT and DOF established a charge-back mechanism to fund the department for the 1996/97 fiscal year. The Administration and the Legislature have adopted pro rata funding for the 1997/98 DOIT budget year.

The Budget Act of 1997 also includes funding to reimburse the DOIT in support of certain project oversight activities conducted by the DOIT. In addition to the specific projects listed in the Budget Act as the Legislature's priority for project oversight, the DOIT has identified additional projects that warrant a closer level of oversight. In most cases, level of risk is a major determinant. The reimbursement amount reflects the cost of project assessments performed by consultants under contract with the DOIT.

Developing a Statewide Plan for Information Technology

State IT Strategic Plan and IT Architecture

California government has experienced its share of IT successes and failures. State government has attempted, succeeded and sometimes failed at automating some of the most complex government operations in the nation. Generally, the state IT enterprise has been primarily devoted to serving the needs of the individual mandated programs. Little consideration as to adaptability, usability and compatibility in a statewide framework was given at the outset of many of these projects.

To provide the kind of direction needed to secure the future for California's citizens, families and businesses, the DOIT developed the *State of California IT Strategic Plan* and recently released it for comment to the ITCC and CITC. The plan provides a vision into the next century, sets strategic directions that will allow that vision to be realized and provides the necessary steps that must be taken to begin the journey into California's future.

For this strategic vision to succeed, it must be acted on. Once enabled, this strategic plan is intended to provide the kind of insight, visionary thinking and policy setting that is necessary to set the course for California's future and ensure that California's taxpayer dollars are used in the most effective and efficient manner possible from a statewide perspective.

The Strategic Plan provides an enterprise-level view of the state's IT resources as they exist today and what they should be tomorrow. The Strategic Plan also provides the vision of what the desired future will be, the framework to make that future possible and offers state government the roadmap which will move California forward.

The Strategic Plan embraces the following vision:

Statewide Information Technology Strategic Plan Developed

The Department of Information Technology has developed a strategic plan that provides an enterprise-level view of the state's information technology resource as it exists today — and what it should be tomorrow.

The strategic plan embraces the following vision:

One state, one IT infrastructure. *The State of California will advocate the use of interoperable, scaleable, interconnected information systems throughout state government to provide flexibility and ease of access to government services to all Californians, thereby contributing to excellence in government and supporting the economic progress in California.*

One state, one IT infrastructure. *The State of California will advocate the use of interoperable, scaleable, interconnected information systems throughout state government to provide flexibility and ease of access to government services to all Californians, thereby contributing to excellence in government and supporting the economic progress in California.*

To support this vision, the Strategic Plan lays out five key strategies and several initiatives that the State of California must undertake to construct this roadmap to the 21st century.

- Strategy #1 — IT policy reform encompassing procurement reform, financial and budgetary control, planning and coordination, and project approval, initiation and oversight.

- Strategy #2 — Infrastructure re-engineering encompassing network consolidation, data center consolidation and business resumption planning.

- Strategy #3 — Statewide IT initiatives encompassing the Year 2000 program, enterprise systems, managing projects and technical architecture.

- Strategy #4 — Strategic initiatives encompassing electronic commerce.

- Strategy #5 — Emerging issues encompassing staff recruitment and retainment, and information privacy and security.

For each of these strategies and supporting initiatives, action steps are specifically outlined in the Strategic Plan, setting the agenda for the next two to three years as California moves toward establishing a consistent and comprehensive statewide vision of what IT will be in the 21st century. The DOIT believes the State of California's IT Strategic Plan will provide the guiding vision and common direction for all state entities to use as they establish individual agency and departmental IT strategic plans.

Enterprise Systems

The State of California spends nearly $2 billion annually on information technology and telecommunications systems. Many of these systems produce, use and process management information that has value to multiple state agencies. However, because the state has a long-term practice of delegating a great deal of administrative responsibility to individual departments, the state has not yet developed a strategic policy for enterprise systems to ensure that they provide the greatest possible benefit to the state's business operations at the least possible cost.

As an increasing number of state departments seek to replace antiquated administrative systems, there is a critical need for a comprehensive strategy to ensure that these new systems will provide ready access to enterprise information. This strategy should include providing a strong foundation for information sharing and collaboration among departments with similar needs, leveraging IT expenditures statewide, reducing redundancy and maximizing return on IT investments.

To meet this need, California's CIO commissioned the Enterprise Systems Subcommittee of the Information Technology Coordinating Council (ITCC) in July 1997 to recommend an overall direction for a statewide strategy for developing and implementing systems that are enterprise-wide in scope.

In September 1997, the Enterprise Systems Subcommittee completed its final report. The highlights of that report include:

- The development of a state Enterprise Systems Strategy provides an excellent opportunity to foster greater collaboration and information sharing among state departments, leading to enhanced effectiveness and efficiency as well as the advent of new enterprise systems.

- New enterprise systems should be flexible and responsive to the needs of the departments they serve, while allowing for compatibility among different systems. Development of a single, centralized system is not recommended.

- Existing statewide IT systems and planned projects, such as CALSTARS and the 21st Century Project, should be included in the Enterprise Systems Strategy. So long as they meet the state's needs, these systems and projects should not be replaced or duplicated and should be used as the foundation for associated enterprise systems.

- Two or three pilot enterprise systems should be designed and implemented to allow evaluation of alternative approaches to state enterprise systems. These pilots must address statewide enterprise data requirements and, if possible, should include one system based on an interagency consortium. They should be implemented and evaluated within 18 months of inception.

- Except for the authorized pilots, a moratorium on development of enterprise systems should be established until select pilots have been implemented, evaluated, and determined to be effective models.

- The state's control agencies should establish a standing committee to coordinate their current and anticipated data requirements among themselves and to continue to define their requirements over the long term.

- A standing committee of the ITCC should be formed to evaluate pilot systems and to further refine and develop the state's Enterprise Systems Strategy.

- A uniform, statewide vendor policy should be developed and enforced to reduce unnecessary costs and redundant purchases.

Efficient IT Infrastructure

Restructuring the State's Data Centers

On July 1, 1997, the DOIT delivered to the Governor and Legislature a report on the data center consolidation study required by the department's enabling legislation entitled *Analysis, Conclusions, and Recommendations on the State of California's Department of Information Technology (DOIT) Data Center Consolidation Study.* The study was performed for the DOIT by the Deloitte & Touche Consulting Group.

This consulting group worked under general subject matter and methodology guidelines provided by the DOIT, but independently developed its findings and recommendations, including assessments of potential savings.

The DOIT, in submitting the final report, included its own specific recommendations and priorities for implementing the recommendations included in the report.

The study provided a preliminary assessment of the feasibility of consolidating the state's information technology assets and specifically included activities conducted by agencies on their own behalf as well as those conducted by data centers. In order to control the scope of the effort, the study focused on those activities that were most likely to prove suitable for consolidation. Therefore, the study did not include office automation and local area networks, which are by nature distributed into the worksites;

applications development, which is generally outsourced under the functional department direction; and data communications networks, which are the subject of a separate consolidation and privatization effort. However, the DOIT did ask Deloitte & Touche to make its recommendations without concern for existing or perceived political and legal barriers and to allow the Governor and Legislature to address such issues during implementation.

The DOIT described the scope of the study and included the specific issues it believed should be addressed in the formal statement of work for the consulting engagement with Deloitte & Touche. The firm used those requirements and its own experience in such efforts to develop a detailed survey instrument.

The DOIT and Deloitte & Touche jointly identified a group of 26 state departments to be the focus of the survey and divided those into three main groups, or tiers. The first tier included the Teale and Health and Welfare Agency Data Centers, which were unique in their provision of services to multiple external departments and in their use of usage-based billing to recover their costs.

The second tier included nine departments that operated mainframe or large centralized computer systems to support internal applications. The remaining survey departments were classified as Tier 3, which maintained large central computing staffs, either for support of internal systems or to augment services provided by one of the Tier 1 consolidated data centers. Survey instruments were designed for each of the three tiers and included both specific questions and requests for certain existing documentation and reports. Tier 3 departments were given the reports to complete independently; Tier 1 and 2 departments were also interviewed by Deloitte & Touche staff.

Following receipt of the surveys, the Deloitte & Touche staff developed a list of key criteria for making any consolidation decision. These criteria included potential cost savings through economies of scale after one-time consolidation costs; governmental policy and legal constraints; business organization alignment; the likelihood of technical distraction or disruption of critical activities through the consolidation effort; the impact of consolidation options on risk management; the service level requirements of departments and the effect consolidation might have on those service levels; changeable conditions; and privacy/security issues. These key issues were used to generate and evaluate a series of potential consolidation options, which were used to focus the analysis of the information presented.

The final report included a series of key findings, and several associated recommendations. Among the findings were:

1. Information technology is a core competency of the state in that there is competence in the areas studied, particularly in the management and operations of large Tier 1 computing environments. Information technology should also be regarded as a core competency of the state in the sense that IT is essential to successfully manage a dynamic, changing environment. This finding is fundamental to any recommendation to maintain state support for data center functions. If Deloitte & Touche had instead found that the large Tier 1 data centers did not support a core competency, divestiture of these functions would have been indicated even if savings could not be identified.

2. The net savings for outsourcing options, after considering all special state requirements, are small. This assessment was based upon an inventory of the essential functions provided to the state by the Tier 1 data centers and the cost of obtaining those same functions through outsourcers. The outsourcer cost estimates were derived from recent winning bids for comparable services by the principal

outsourcing providers. The study did also find, however, that certain core rates of the Tier 1 data centers, such as for mainframe processing and data storage, were substantially greater than those of outsourcing providers, due largely to the recovery of costs for non-billed services to state departments. The data centers have begun working to modify their rate structures to align them more closely with competitive systems. This has already resulted in substantial rate decreases for Teale Data Center customers.

3. Significant savings and concentration of key resources can be obtained through the consolidation of all state IBM-compatible mainframe functions into the existing Tier 1 (HWDC and Teale) data centers. Further savings could be achieved by consolidating the Teale and Health and Welfare Data Centers into a single facility, but the study identified risks associated with this option that Deloitte & Touche believed might outweigh the potential benefits.

4. The state has an experienced but aging workforce supporting critical legacy mainframe systems. The knowledge of this workforce, particularly knowledge that is state-specific, must be preserved beyond the point at which critical staff retire. In newer, non-legacy environments, the state has experienced difficulty in attracting, hiring and retaining skilled technical staff, largely because of existing job classification and salary limitations. The DOIT believes that this issue may be the most compelling strategic reason for aggressive consolidation efforts: the cost of obtaining adequate staff for multiple data centers may become prohibitive during the next decade.

5. Year 2000 problems present a serious risk to state government and will require substantial efforts by data center personnel if they are to be successfully addressed. The DOIT and Deloitte & Touche agreed that this finding, however critical, affects only the timing, not the feasibility, of consolidation.

6. The state's existing operational recovery plans for information systems are weak; few have been successfully tested. Departments need to commit staff and resources to address the basic steps of business impact analysis, critical application identification, recovery plan development for critical applications and testing. The study further found that the smaller the department's information technology staff and function, the poorer their operational recovery and information security programs. The DOIT also specifically asked Deloitte & Touche to evaluate the suitability as to consolidation destinations of the existing Teale and Health and Welfare Agency Data Centers. Deloitte & Touche recommended that neither site be used for any potential consolidation of the two centers and commented that such consolidation would "absolutely force the construction of a new data processing facility outside of the Sacramento floodplain, as a necessary risk minimization step."

Deloitte & Touche then made a series of recommendations based upon those findings and the criteria-based evaluation of possible options. The principal recommendations included:

1. Pursue consolidation into the Teale Data Center of those IBM-compatible mainframe functions that remain outside of the Tier 1 data centers. These facilities include those owned and operated by the Franchise Tax Board, State Controller's Office, Public Employees Retirement System, California State Lottery and State Treasurer's Office. The study estimates that the consolidation of all of these environments would result in a savings to those departments after an initial investment to effect the consolidation. The study also anticipates that additional savings will accrue to all other users of the Teale Data Center through improved economies of scale

resulting from these consolidations. The study recommends that the state regard the consolidation of the Teale and Health and Welfare Data Centers as a long-term option to be considered only after issues of operational recovery preparation and testing, business function support, technical disruption and Year 2000 problems have been addressed, and only if financial benefits are identified that justify the risk and effort of consolidation. The study identifies potential savings after an initial investment to complete the consolidation of the two tier 1 data centers.

2. Pursue conversion of either the Teale or the Health and Welfare Agency Data Center to a state-owned private corporation dedicated to providing data processing services to California government. This effort is intended to provide relief from restrictive state budgetary and planning cycles, personnel policies and salary structures which limit the state's ability to recruit and retain appropriately skilled technicians and managers.

3. Consider the full costs of non-mainframe activities, including business continuity and operational recovery, security and systems management, when evaluating new proposals for such activities and either centralize or distribute them as appropriate. Do not centralize existing non-mainframe systems unless dictated by changed business requirements for those activities.

4. Establish centers of expertise for certain functions that require specialized technical and management skills, such as imaging, Geographic Information Systems, public access services and specialized operating systems environments.

5. Do not undertake any consolidation activity until all critical Year 2000 problems involving the affected data processing facilities and staffs have been resolved.

Finally, the DOIT identified the specific actions it would take in implementing the Deloitte & Touche study recommendations. These were developed with guidance from a steering committee which included representatives of the Health and Welfare, Business, Transportation and Housing, and State and Consumer Services Agencies, the Department of Finance, and the Office of Planning and Research. Recommended actions include:

1. The DOIT will request each agency that owns a Tier 2 IBM-compatible mainframe data processing facility to develop for consideration plans to transfer those functions to the Teale Data Center. These conversions would not take place until after all critical Year 2000 issues have been addressed to ensure that neither the data centers nor the Tier 2 agencies are disrupted in their efforts to meet Year 2000 requirements.

2. The DOIT will request the Teale Data Center to take immediate steps to acquire a data processing facility suitable for its existing workload and anticipated growth. This facility should not initially be constructed to support the further consolidation of the Health and Welfare Agency Data Center, but should be designed to allow future expansion without excessive cost or disruption to existing operations.

3. Initiation of an effort to develop a plan to convert the Teale Data Center to a private, state-owned corporation by 2002.

4. The DOIT will work with state agencies to begin an aggressive program to identify the business continuity requirements for all functions supported by the state data centers and departmental computing facilities, and to implement and test suitable operational recovery plans for all such functions.

5. Through the FSR process, the DOIT will require that all new non-mainframe systems

(excluding those used for local area network and office automation functions) be sited at the Health and Welfare Agency or Teale Data Centers, as appropriate for the existing business alignments of those data centers, unless the departments proposing such new systems are able to identify specific business justifications for alternate siting.

6. The DOIT will reconsider the consolidation of the Health and Welfare Agency Data Center with the Teale Data Center only if the corporatization of the Teale Data Center has demonstrated the expected benefits of that corporatization.

While the need to postpone many activities until completion of Year 2000 remediation severely limits the ability of the DOIT to make dramatic progress on consolidation, the DOIT has moved aggressively to integrate the consolidation vision clarified through this study into state information technology and practice. The DOIT has drafted, and has enforced in all feasibility study reports requesting new information technology projects, several of the policies recommended by the study.

These include a requirement that any proposed new centralized computing facility be located at one of the existing consolidated data centers unless both compelling business requirements exist for alternate siting, and the proposing department has identified and is able to support the operational recovery and security requirements of the proposed system. The DOIT is reviewing all new infrastructure investments by the Tier 1 and Tier 2 data centers recommended for consolidation to ensure that any such investments that must be made before consolidation are not inconsistent with a future, single, consolidated environment. The DOIT has also begun to require that the Teale and Health and Welfare Agency Data Centers perform long-term planning in cooperation with one another, instead of independently as they have in the past.

The DOIT is particularly concerned with the need to develop new skill sets and support capabilities for evolving technical requirements. In recognition of the increasing cost and difficulty of recruiting and training technical personnel with specialized skills, the DOIT is working with the consolidated data centers to limit the development of new centers of expertise to one or two concentrated facilities. Such functions have so far included UNIX-based system support, frame-relay networking and multi-protocol router management.

The DOIT has retained consulting assistance to conduct a more detailed analysis of the operational recovery plans filed with the DOIT by state agencies. This analysis is intended to help the DOIT to identify more specifically the general deficiencies with this planning noted in the data center consolidation study, and to help the DOIT to determine the activities and policy improvements necessary to ensure recovery of critical systems. The DOIT has also been working with the Business, Housing and Transportation Agency, along with the Teale Data Center, to develop a suitable plan for replacing the existing Teale facility, largely in order to address the critical availability and disaster exposures associated with that facility.

Overall, the Deloitte & Touche study found that compared with other states, California's data centers were relatively well consolidated under the framework of the 1972 data center legislation. Moreover, the study found that the quality and cost of service associated with the Teale and Health and Welfare Agency Data Centers are at least comparable to those of the private sector. Nonetheless, the study found considerable avenues for improvement, particularly in those environments which have remained or recently developed outside of those data centers. Finally, the study indicated that the consequences of failing to consolidate further, in terms of personnel costs, service levels, and security and disaster exposures, are likely to become more severe during the next decade.

The DOIT is ensuring that the state's distributed data center environment does not become more fragmented while it waits for completion of Year 2000 efforts before undertaking aggressive consolidation. More importantly, the DOIT is working with state agencies to correct the other existing and potential problems with its data center infrastructure, and to do so with policy-based initiatives that will ensure a lasting benefit.

Privatizing The State's Telecommunications Networks

In December 1996, the DOIT, in partnership with the Department of General Services (DGS) Telecommunications Division, released a new strategic plan for the state's networks. This report, entitled *California Integrated Information Network: A Strategic Plan for CALNET and All State Telecommunications Networks*, made a series of findings regarding California Network (CALNET) and the state's other telecommunications networks, and outlined a strategy to address the problems with CALNET while establishing a process to achieve real network consolidation.

During the past year, the DOIT and the DGS have made substantial progress toward implementing that strategic plan. The primary goal of that plan — the privatization of CALNET and the associated network services — is scheduled for completion during the first half of 1998. The DOIT is also well underway in its efforts to coordinate the state's telecommunications into a single business entity. The goal is to obtain highly competitive pricing and an unprecedented quality of service that should be made available to the State of California, which will be California's single largest telecommunications customer.

In January 1997, the DOIT issued a Management Memo (MM 97-01) requiring state agencies to use CALNET or DGS Telecommunications Division contract services unless specifically exempted by the DOIT. The intent was to maximize the value of the upcoming privatization procurement by establishing the state as a single purchasing entity for telecommunications services. The state currently acquires the majority of its telecommunications services through contracts administered by the DGS. However, many departments contract directly with vendors for specific services. In some cases, these direct contracts are necessary to obtain services which are not available through CALNET or DGS contracts. In other situations, the department either prefers an alternate vendor or obtains more attractive pricing. While it may seem beneficial to allow state entities to obtain the best pricing they can find, these practices may actually substantially increase the state's overall telecommunications costs. Vendors could be reluctant to offer highly competitive pricing for blanket state contracts if they fear that selected and usually more profitable portions remain available to vendors who either lost or chose not to participate in the general contract procurement.

The DOIT has also worked with state departments so that interim service contracts and other state data communication and telecommunication activities are structured to ensure the ability to adapt to the California Integrated Information Network (CIIN) privatized telecommunications environment once that procurement and implementation are completed.

The procurement to privatize CALNET and to obtain a single source for the state's telecommunications service requirements is also proceeding as planned. The DGS conducted a Request for Information (RFI) process during the spring of 1997 to solicit industry comments on the proposed procurement, and to obtain specific comment on certain technical and regulatory issues. Of 12 vendors who participated in this process, formal responses were received from 10.

The DGS, with the concurrence of the DOIT and in response to the unanimous RFI response preference, chose to conduct this procurement using alternative processes to allow potential bidders flexibility in the solution they offered. This process began in September 1997 with the selection of potential business partners who possessed the technical and financial ability to meet the state's requirements. A total of six vendors were selected through that process.

Those business partners received a Solicitation for Conceptual Proposals in October 1997. This document, which replaces the more technically restrictive Request For Proposals (RFP) used in standard procurements, generally included three types of specifications.

The first specification is a group of essential services, primarily those necessary to replace the services provided through the existing CALNET infrastructure that the successful business partner must provide. Secondly, the state specifies a group of optional services, which the prospective business partner may choose not to provide, but which are important to the state and will increase the value of a proposal during evaluation. Finally, prospective business partners may offer pricing for any other telecommunications services that it wishes to offer to the state through this procurement. Prospective business partners are allowed considerable latitude in the manner in which they meet the requirements, which are largely described in business function terms.

Draft Conceptual Proposals, including proposed contract language, were due in early November 1997. The DGS, with the assistance of key state telecommunications users, will continue discussions through January 20, 1998, with business partners to assist in correcting problems with their draft proposals. The DGS will also conduct parallel contract negotiations with each prospective business partner through January 1998.

Contract award is planned for the first half of 1998. The actual implementation schedule will be developed by the prospective business partners during the proposal phase, and the rate of conversion, and consequent value to the state, will be a subject of the overall evaluation. It is required, however, that the winning partner complete the removal of CALNET equipment from the state's San Francisco facility before November 1998, and from Los Angeles by December 1999.

While all of the components and details of the CIIN environment are not yet known, including the proposed date when cutover to that environment will be completed, several results are apparent and clearly worthwhile. The state will change its approach to obtaining telecommunications services from one involving the ownership and operation of network infrastructure to one where services are obtained from vendors using the infrastructure they have built and maintained for their general customer base. The state's CALNET network will cease to exist, as will most of the independent telecommunications networks owned and operated by individual state agencies and by the data centers. Most importantly, the state will competitively obtain telecommunications goods and services with the quality, price and flexibility appropriate for the largest customer in the state.

Protecting State Information

Disaster Recovery

Disaster preparedness has long been regarded in both industry and government as a technical problem. The obvious vulnerability of mainframe computer installations led their owners to pioneer the disciplines of availability, continuity and disaster recovery planning and preparation.

Yet disasters will impact business systems and information technology systems alike. Just as it makes no sense to recover an information

technology system without recovering the rest of the components of the business systems it supports, it makes no sense to recover business functions supported by information technology without planning to recover critical government functions that do not rely on information technology. While the DOIT is responsible for state agency disaster recovery planning with respect to information technology, it is increasingly clear that the state must involve business program management in planning to ensure that its critical functions will survive, or at least be recoverable after, a disaster.

Even within the IT environment, where the state has required disaster recovery planning for over a decade, the level of preparedness is disturbingly low. As a part of the Data Center Consolidation Study performed for the DOIT by the Deloitte & Touche Consulting Group, the DOIT asked for an assessment of the disaster recovery planning and preparation at the 25 subject data centers and departmental computing facilities. In their final report from that study, Deloitte & Touche commented that:

> "[T]here are few operational recovery plans that have been successfully tested... Departments need to commit staff and resources to address the basic steps of business impact analysis, critical application identification, recovery plan development for critical applications, and testing involving participation of user departments... Our study indicates that the most technically advanced methods for security management and recovery management are found in the largest installations, and that sophisticated methods are rarely found in small computing facilities."

That report included a recommendation that the state regularly evaluate the existing mid-range computing facilities which are not consolidated at a data center and to consider relocation when operational recovery capabilities, among others, are found to be weak. The report further recommended that the state include an understanding that centralization allows improved institutional skill and facility support for operational recovery when planning the location of new facilities. Finally, the report identified the weakness of existing operational recovery plans for critical data center-based applications as a barrier to the consolidation of the Teale and Health and Welfare Agency Data Centers and recommended that consolidation occur only after those plans are in place, successfully tested and supported on an ongoing basis.

Alarmed at this general assessment of the information technology operational recovery plans at the state's largest facilities, the DOIT commissioned Deloitte & Touche to perform a review of all of the 77 operational recovery plans filed at the DOIT. Not surprisingly, the addition of 52 smaller organizations to the review did not brighten the picture. Deloitte & Touche evaluated each plan for nine basic components, including:

- Data backup provisions;
- Equipment replacement or substitution;
- Site replacement or substitution;
- Periodic plan testing;
- Document recovery procedures;
- Understanding of business priorities for recovery;
- Detailed hardware and software inventories;
- Recovery plan maintenance procedures; and
- Clear assignment of responsibility for plan management and execution.

For each component, Deloitte & Touche assessed whether the plan indicated that the capability was in place and appeared adequate, was partially in place or under development, or was not in place or did not appear adequate. Deloitte & Touche also estimated the actual time it would probably take to recover the critical systems identified in each plan, and compared this expected recovery time for the different lines of government business represented by each agency. Finally, they identified agencies whose plans included potentially fatal flaws, exposing their mission critical systems to a "special risk" that their mission critical systems may not be recoverable. Deloitte & Touche's conclusions included:

- Approximately 53 percent of the agencies are at special risk of not recovering their mission critical systems;
- Nearly 57 percent of the agencies would require more than 14 days to recover their mission-critical systems;
- Approximately 70 percent of the agencies have incomplete plans for data backup and recovery and 13 percent would probably not be recoverable at all due to inadequate data backup and restore measures;
- Two-thirds of the plans reflect a poor-to-fair understanding of their agency's business priorities;
- Only one agency in six is testing its plans and documenting results on a regular basis; and
- Only three of the 77 plans include complete, detailed recovery procedures.

The line-of-business comparison did not indicate that the state is doing a better job with the most essential services: Only three agencies will recover in three days or less; none of those are in law enforcement, emergency services or fiscal and revenue collection organizations. Of the 13 agencies involved in the most time-critical functions (law enforcement, emergency services, fiscal and revenue collection, transportation and corrections), only three have plans that will allow recovery in less than 14 days.

The DOIT has initiated several efforts to address this situation. In 1996, the DOIT commissioned the development of a documented methodology that state agencies can use to conduct a business impact analysis. This essential first step to any disaster preparations involves the identification of mission critical business program functions, and the maximum acceptable outage to those functions. The analysis must determine how long supporting processes, including information technology systems, can be interrupted before the business program function will experience an unacceptably long outage. This information can then be used to develop, test and maintain operational recovery plans. This business impact analysis methodology is available at no cost to state agencies which wish to use it to assist their planning effort; several state agencies have already adopted the tool.

To address a key flaw in the filed operational recovery reports, the DOIT will issue a Management Memo and is updating the relevant State Administrative Manual (SAM) sections to require that all operational recovery plans include provision for testing each testable component of the plan every three years, and to identify alternative verification methods for components that cannot feasibly be tested. Agencies will be required to include the results of all tests conducted during the prior year in the annual plan updates filed with the DOIT. The SAM changes will also include clarification of the requirements for business impact analyses to specify that the maximum acceptable outage for each information technology system must be identified and based upon the maximum acceptable outage for the underlying business system.

The DOIT has also begun to enforce policies for new projects. In accordance with the recommendations of the Data Center Consolidation Study, the DOIT requires that departments must locate new systems at existing consolidated data centers, which generally maintain the most sophisticated disaster preparedness capabilities. Departments are exempted only if they can show compelling business requirements for alternate siting, and have included provisions for implementing and maintaining necessary security and operational recovery provisions at the alternate site. The DOIT is also requiring that new systems that will support mission critical applications include appropriate provision for operational recovery.

In the past year, there has been significant improvement in the operational recovery readiness of some departments. The Franchise Tax Board and Board of Equalization have completed business impact analyses, and the Franchise Tax Board has submitted an FSR to obtain out-of-state facilities and services for critical application recovery. The Department of Motor Vehicles has begun testing its own use of that service and obtained a group contract administered by the Teale Data Center. The Department of Justice has also obtained DOIT approval for its plan to recover its California Law Enforcement Telecommunications System (CLETS) network using an alternate facility in Southern California. The Teale Data Center is proceeding to relocate its facility, site of information technology systems supporting over half of the state's departments, to a location less threatened by flood or transportation disasters.

However important, these improvements in the state's information technology disaster preparedness are incremental; dramatic improvements are required. Many urban locations in California are estimated to face a threat of major earthquake within five years or less. Much of Sacramento, the seat of government, is estimated to face a similar threat of flooding. The potential for terrorism or civil disturbance, either of which is likely to target government offices, is steadily increasing. Fire is a constant threat to every facility. Even a toxic spill from a transportation accident can render a site unusable indefinitely, even if undamaged.

The state should consider disasters a certainty within its planning horizon and develop preparations with the expectation that they will be needed. Many private entities expend 1 percent or more of their information technology budget on disaster preparedness for their critical computer systems; the state does not spend even a tenth of that amount on its preparations. The DOIT will continue to work with departments to develop prudent, viable recovery plans, but these efforts will fall well short, and the state's critical systems will remain exposed to lengthy interruption or outright destruction, unless the state makes disaster preparedness a business responsibility instead of a technology afterthought.

Information Security

The DOIT is broadly responsible for establishing, monitoring and enforcing information technology security policies and practices in California state government. The most important tools for executing this responsibility are the DOIT's authority to review and approve new IT projects and the requirement that departments file reports of IT security incidents with the DOIT. The DOIT has taken several steps during the past year to improve the effectiveness with which it applies these tools. The DOIT believes that these efforts, while necessarily incremental, will enable rapid improvements in the security preparedness of the state.

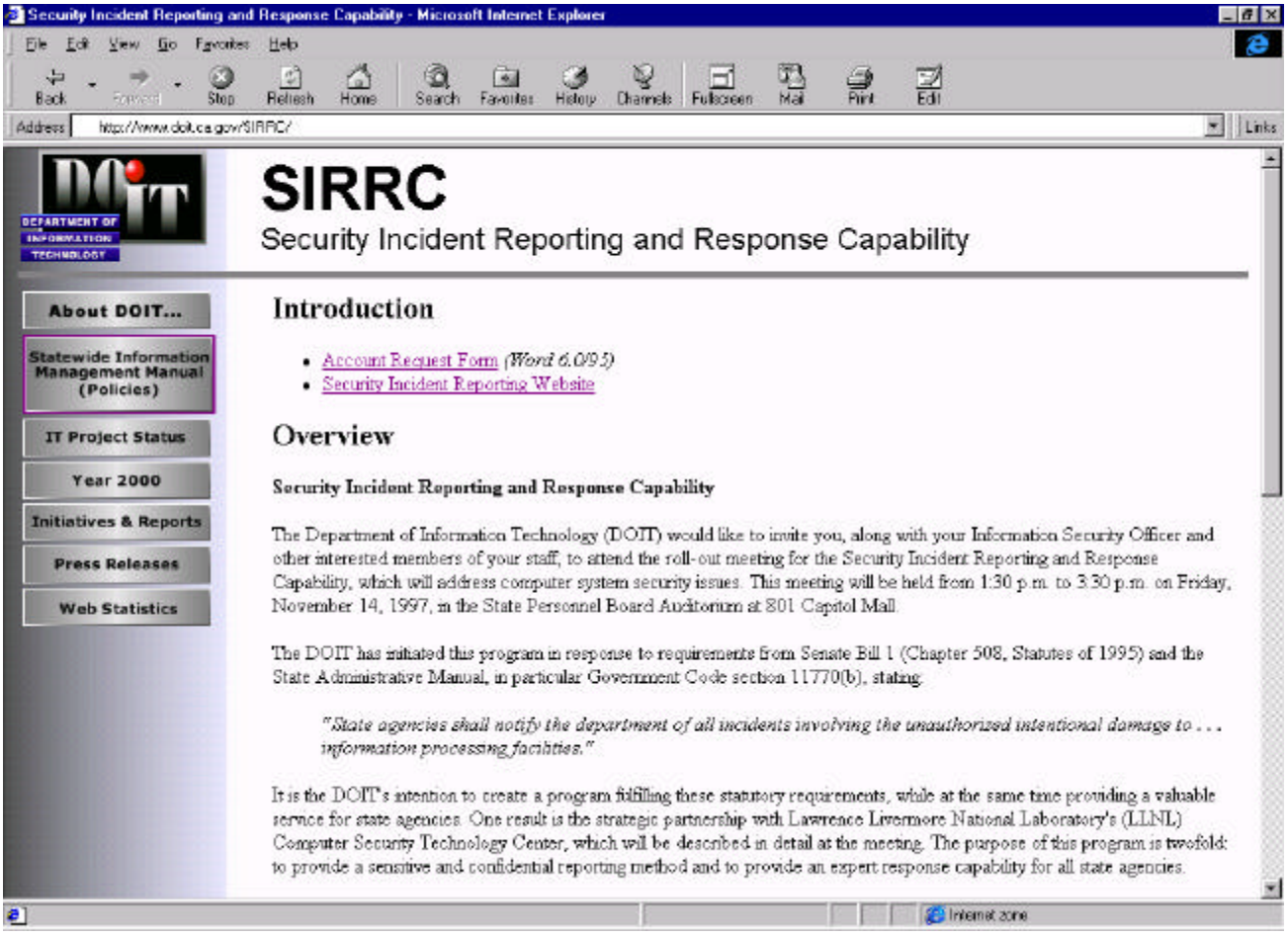
The DOIT has begun to require that proposals for new IT projects include specific provision for information security. This requirement has been selectively applied during

the past year to projects which include particular risk, such as when the information generated is sensitive or confidential, or when components of the proposed system will cause a substantial exposure for attack. The DOIT has focused attention on ensuring that departments are aware of the special risks associated with internetworking and the increasing sophistication of potential attackers, and that their projects are designed appropriately.

In the next year, the DOIT will publish more general standards for the IT security requirements for new projects. The DOIT will require that departments evaluate the security risks presented by new IT projects, and that each project contains a level of security mitigation so that the project does not add a level of security exposure that is not acceptable to the business managers of the supported function. The DOIT is also developing minimum security measures that must be provided for all projects; these will include low-cost, high-benefit activities, and efforts to address exposures to known, active threats.

In order to gain a greater understanding of the threats encountered by state government, and to provide assistance to departments in responding to actual attacks, the DOIT has contracted with the federal Department of Energy's Lawrence Livermore Laboratories Security Incident Technology Center (SITC) to develop an incident reporting and response capability for the state.

Departments are currently required to file reports of security incidents with the DOIT, but this reporting has been sporadic and the accumulated reports of little value to the state. The SITC has developed a secure, encrypted system to allow departments to file online reports of security incidents. The SITC will provide monthly summaries of these incidents to state departments, including experienced attack



methods, emerging threats, preventive measures and popular targets. The SITC will also provide detailed information to the DOIT that it can use to adapt policies to changing attack and prevention technologies. The SITC will work with the DOIT to issue emergency bulletins, as when a new attack method has come into use, or when a state resource has been identified in attacker literature and bulletin boards. Finally, the SITC will provide immediate assistance to departments in responding to attacks, including technical direction on identifying the level of compromise and on closing the exposure. This service became available in November 1997, and will be provided by the DOIT to state departments at no charge.

The DOIT has been working with departmental and legislative staffs who are developing plans to require the use of new technologies for state business. In particular, the DOIT has been involved in efforts to use electronic means to deliver government services, and to obtain and publish information. The DOIT maintains current information regarding the availability and effectiveness of security and confidentiality methods for electronic commerce and Internet communications, and is assisting project and policy planners to ensure that proposals for new requirements include prudent and reasonable consideration of security exposures and capabilities. The DOIT has been particularly concerned with the ability of currently-available technologies and services to support the authentication and non-repudiation requirements for electronic delivery of certain government services. These, and other issues of security relative to electronic provision of government services, are discussed in more detail in the article on electronic government that is also in this annual report.

In general, the DOIT is keenly aware of the special nature of government and its custodianship of confidential or sensitive information about its citizens, business and organizations. Often the issues of security for IT systems are similar to those for manual processes they supplant and can be addressed through the same types of physical security and staff procedures. In other cases, particularly when computers are connected to large open networks, the use of information technology to store, process and transmit information presents new and challenging security risks. Either way, the DOIT is working diligently with vendors, state departments and technologists to ensure that the state's IT systems are conceived, constructed and maintained so that the state does not negligently or ignorantly risk its public trust.

Improving State Management of Information Technology

Addressing Risk: Independent Oversight

Independent, private sector oversight teams are now in place for the state's largest and most complicated IT projects. This constitutes a level of independent oversight never before seen in the history of the state's information technology program.

The DOIT has developed a sophisticated Risk Assessment Model (RAM) that provides a tangible evaluation of project risk ***before*** initiation and throughout the project life cycle, enabling mitigation plans to be developed. Created through a comparison of several models used in the private sector, the DOIT RAM has been improved and was used on many state IT projects in 1997.

Via a data base application developed by the DOIT, the Legislature now has access through the World Wide Web (www.doit.ca.gov) to continuously updated information about California's IT projects, including summary descriptions, managers, budgets, schedules and other critical data.

The use of independent project oversight contracts has not only provided many state departments valuable assistance in their efforts to implement IT projects successfully, but has been of particular benefit to the state with respect to projects which have encountered serious difficulty and have had to be terminated.

Reducing the Risk of Failure

The risk associated with implementing state IT projects remains in many instances very high. Risk will always be high for complex projects. Moreover, this risk is inherent in IT projects and is by no means unique to California state government. As noted in our previous annual report, research indicates that over 31 percent of the approximately 175,000 information technology development projects in the United States will be canceled prior to completion. The research also indicates that 52 percent of projects nationwide will cost almost twice as much as their original budgets, while only 16.2 percent of projects will be completed on-time and on-budget. In large companies — California state government falls into this category — only 9 percent of projects will complete on-time and on-budget. In 1995, American companies and governments spent $81 billion on canceled software projects.

These statistics demonstrate that the risk of IT project failure is quite real in all sectors, and therefore some level of failure can be anticipated; however, the goal of the DOIT's oversight effort is to minimize the potential for failure through a combination of methods, so that over time California achieves an increasingly higher ratio of project success, with a corresponding diminution in outright failures. Accordingly, the DOIT has focused on the following primary instruments for mitigating risk:

- ❖ Project initiation and approval;
- ❖ Independent project oversight;

- Risk Assessment Modeling (RAM);
- Risk mitigation planning; and
- Online project tracking information.

In addition, the DOIT plans to improve risk mitigation by:

- Improving the state's model contract for IT projects;
- Requiring the use of external experts to assist state IT projects in the areas of project management, contract management and contract drafting and negotiation; and
- Establishing a peer review process to subject major projects to periodic reviews by a panel of experts, which may include a mix of state and private sector individuals.

Project Initiation and Approval

The DOIT has been given responsibility throughout the project lifecycle for enforcing practices to increase the likelihood of project success. In addition, the DOIT is required to add an enterprise perspective to planning, implementing and operating state IT projects. These goals require the DOIT to perform tasks in support of project initiation which are substantially different than those performed in the past. Consequently, substantial policy reform is required in the areas of project initiation and approval.

The DOIT, in cooperation with the Department of Finance (DOF), defined a new methodology governing the consideration of approval and funding of IT-related proposals. This methodology was published in a report to the Joint Legislative Budget Committee in December 1997, entitled *State of California Information Technology Project Initiation and Approval Report*.

The purpose of the new methodology was to: (1) establish a uniform format for use by state departments and agencies in identifying and reporting their respective IT project needs and statuses, and (2) enhance the coordination between the DOIT and the DOF regarding the consideration of requests for funding IT projects.

The new methodology significantly changed the previous project initiation and approval process in the following manner:

- A sequential process was established for submission and review of IT project proposals by the DOIT and the DOF;
- The DOIT functions as the "conduit" between departments and the DOF with respect to IT project proposal reviews and approvals;
- A "pre-review" of IT project proposals is conducted among the DOIT, departments and the DOF prior to full Feasibility Study Report (FSR) development;
- The DOIT conducts all technology-associated project proposal reviews;
- Upon DOIT approval, the DOIT acts as an "advocate" for agencies and departments throughout the budget process; and
- The DOIT is committed to certain time frames for its reviews.

In addition, the DOIT and the DOF developed clear definitions of roles and responsibilities for departments, agencies, the DOIT and the DOF. Departments are

responsible for ensuring that departmental IT solutions are in alignment with the long and short term strategic goals of their respective program areas, and ensuring that the solution is aligned with the state's overall direction, operation and deployment of IT as established by the DOIT. Departments are responsible for ensuring that their IT activities are in compliance with state IT policies, standards and reporting requirements.

Under the new methodology, the agency becomes responsible for ensuring that departmental project proposals conform to the business and IT strategies and policies of the agency and the Administration. As with the department role, the agency is responsible for ensuring that all departments within its purview are properly deploying technology in alignment with the business and IT strategic plans for the individual departments and the agency as a whole.

The DOIT performs three major roles for administering and overseeing state IT: advocate, gatekeeper and control agency. As the advocate, the DOIT is responsible for advocating the advancement of IT in state government operations. The DOIT will work closely with departments and agencies in advancing the use of technology to best meet the needs of California's citizens and businesses by making government more efficient. As the Administration's technology advocate, the DOIT will represent departments and agencies in resolving fiscal issues with the DOF concerning the deployment of IT in state government operations. The DOIT will also represent the Administration before the Legislature in hearings and other events as they relate to the state's IT activities.

As the gatekeeper, the DOIT will be responsible for ensuring that departments and agencies expend effort and resources to develop only project requests that are properly aligned with the state's overall IT strategies, infrastructure and policies.

As the control agency, the DOIT will be responsible for reviewing, supporting and approving all state IT activities. The DOIT will be responsible for supporting and approving only those state IT activities that are aligned with state policies, strategies, architectures and standards. The DOIT will also provide guidance to departments and agencies in modifying project proposals to align them with state policies and strategies, or will deny efforts that cannot be so aligned.

The DOF will be responsible for assessing and funding projects in light of budget policy priorities, investment value and merits to the operation of state programs. The DOF's review is based on an acceptance of the DOIT's review of the project with respect to the technology solution. The DOF's review will focus on the stated business/program benefits, and on the completeness and accuracy of cost and resource assessments. The DOF may return projects to the DOIT based on these criteria. The DOIT, in conjunction with the affected department, may submit a modified project proposal for reconsideration.

The DOIT believes that the new methodology, coupled with the clearly defined roles and responsibilities, will be of net benefit to state government and should facilitate the efforts of state departments and agencies to apply IT as an effective solution to satisfying business requirements.

To complete the implementation of the uniform process for project initiation, approval and change, the DOIT will continue to undertake a number of steps. It is the DOIT's and the DOF's intent that the process be in place for budget development and enactment of the Governor's 1999/2000 budget. This requires that: (1) all policies and guidelines supporting the process must be in place by January 1998; (2) training for the revised policies and guidelines be given jointly by the DOIT and the DOF by

March 1998; and (3) departments and agencies must adhere to the revised policies and guidelines by May 1998. The results of the revised process and supporting policies and guidelines will be reported in the DOIT's Annual Report to the Legislature in December 1998.

Independent Project Oversight

The objective of project oversight is to ensure that a department's projects are implemented within the planned schedule and budget. Accordingly, proper oversight demands that the earliest possible notification be given regarding potential impediments to progress. In this way, mitigation actions can be taken to reduce the risk of project failure. The most effective project oversight is applied in a condition of independence (i.e., the individuals performing project oversight must be detached from the organizational chain of command of the project managers). In this manner, they retain their impartiality and their findings are less prejudiced.

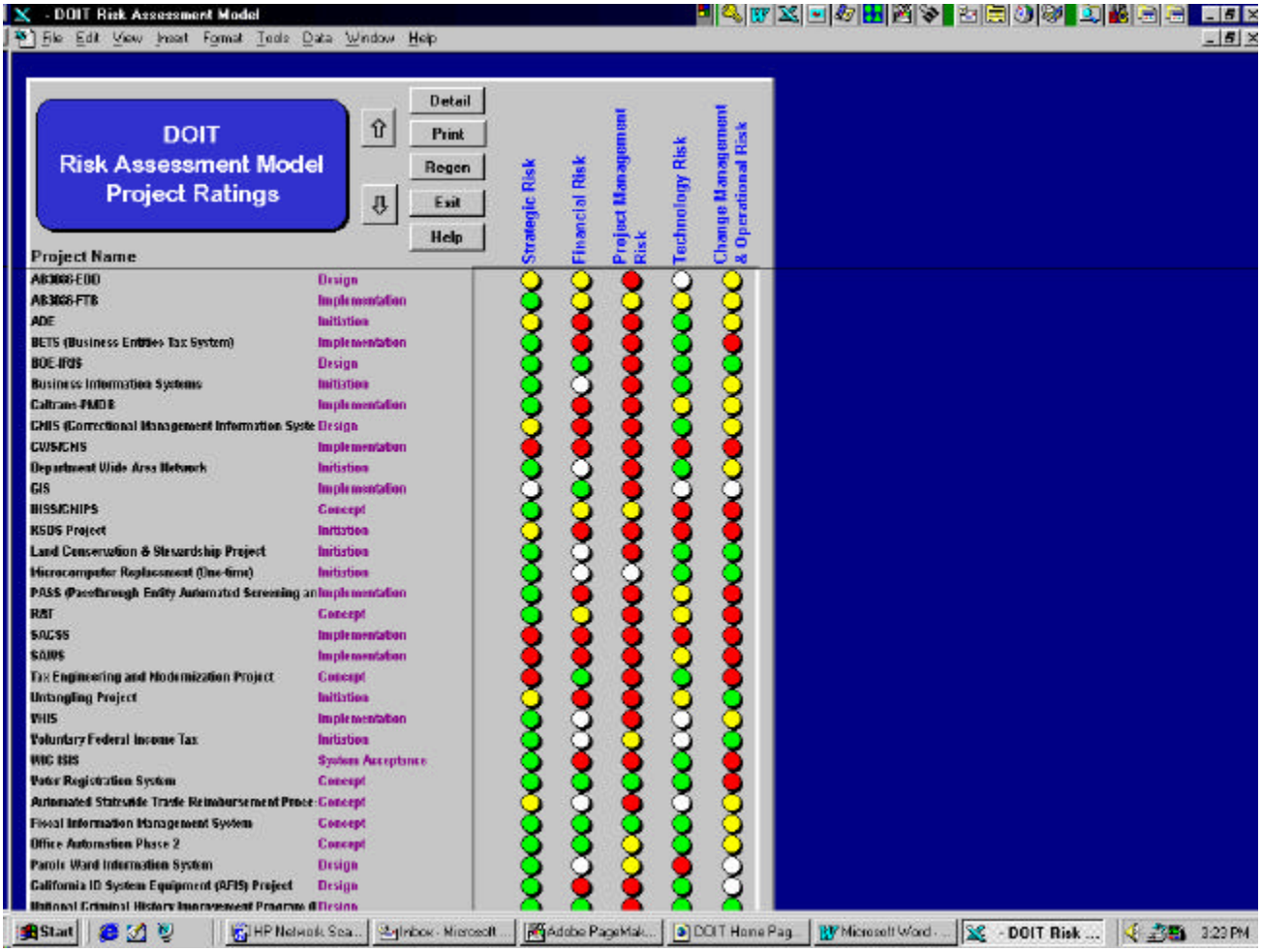
While the objective of employing independent project oversight is to help ensure that state IT projects are implemented successfully, effective independent oversight is also important with respect to projects which experience serious difficulties and have to be terminated. In such cases, independent oversight helps to protect the state's interests by bringing to the project development process skilled expertise which helps the state to avoid contractual breaches while at the same time documenting a contractor's contractual performance. For projects which result in litigation, the information developed by independent project oversight contractors, and their expert testimony, may provide the state a measure of protection which it has not previously enjoyed.

Independent project oversight employs a variety of management and technical review methods based upon professionally recognized processes or standards promulgated by organizations such as:

- Comptroller General [Performance Auditing (non-financial auditing) used by all public audit agencies and CPA firms];
- American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) related to management consultants 'work; and
- American National Standards Institute (ANSI), including standard 1012 governing software and systems independent verification and validation (IV&V).

Independent oversight is a common practice in the private sector. However, utilization of independent oversight has not historically been universally accepted by state government IT managers. Some argue that oversight is the responsibility of the project manager and that hiring independent oversight contractors squanders scarce state funds that could otherwise be used to reduce the cost or expand the scope of the project. Nevertheless, the CIO has made the policy decision that the investment in independent oversight on major IT projects is essential to reducing the state's exposure to risk. As a result, in 1997, private-sector, independent oversight teams were put in place on a number of the state's major IT projects. Most state IT project plans and budgets now contain provisions for independent project oversight. The independent oversight teams report to the agency project manager and to the DOIT and will help ensure that projects are on-time, on-budget and meet the specifications laid out in the contract.

In most cases, the independent oversight contractors are employed at the beginning of the project and perform a variety of management and technical oversight activities. These activities are performed in parallel with the development effort, which allows the oversight contractor to identify issues and recommend corrective actions early in the life cycle. As changes are identified,



the oversight contractor can quickly assess the impact to the existing project plan and schedule and recommend changes to eliminate or minimize the impact.

To facilitate the oversight process, the DOIT has initiated a project to refine and enhance its existing Project Oversight Methodology to incorporate "best practices" and "lessons learned" in other oversight programs, including programs used by private sector, independent oversight teams and other states. This enhanced version of the methodology will include guidelines to assist departments in meeting the DOIT's oversight requirements and in acquiring appropriate oversight services. It is anticipated that the enhanced version of the methodology will be released in the Spring of 1998.

Risk Assessment Model

One of the primary objectives of the DOIT has been to mitigate risk on IT projects. When the department was created, no tool existed to gauge the risk associated with any given project.

To accomplish this, the state needed a Risk Assessment Model (RAM). RAM is a term used to describe the arithmetic measurement of the level of potential risk associated with various components or categories common to all projects. In other words, a RAM, by assessing various factors relating to a project, can identify those riskier aspects or categories, which may then be mitigated or resolved by project managers. A formal risk assessment performed during the early stages of project planning helps to identify major

areas of project risk, and may even be cause to cancel the project outright. Periodic assessment after project initiation provides tangible benchmarks for project managers and the DOIT to evaluate and plan appropriate remedial efforts if necessary.

In order to determine the appropriate risk assessment model for the DOIT, an evaluation was performed on various RAMs in use throughout the industry. The comparison yielded several common major categories of risk which were being evaluated by these tools:

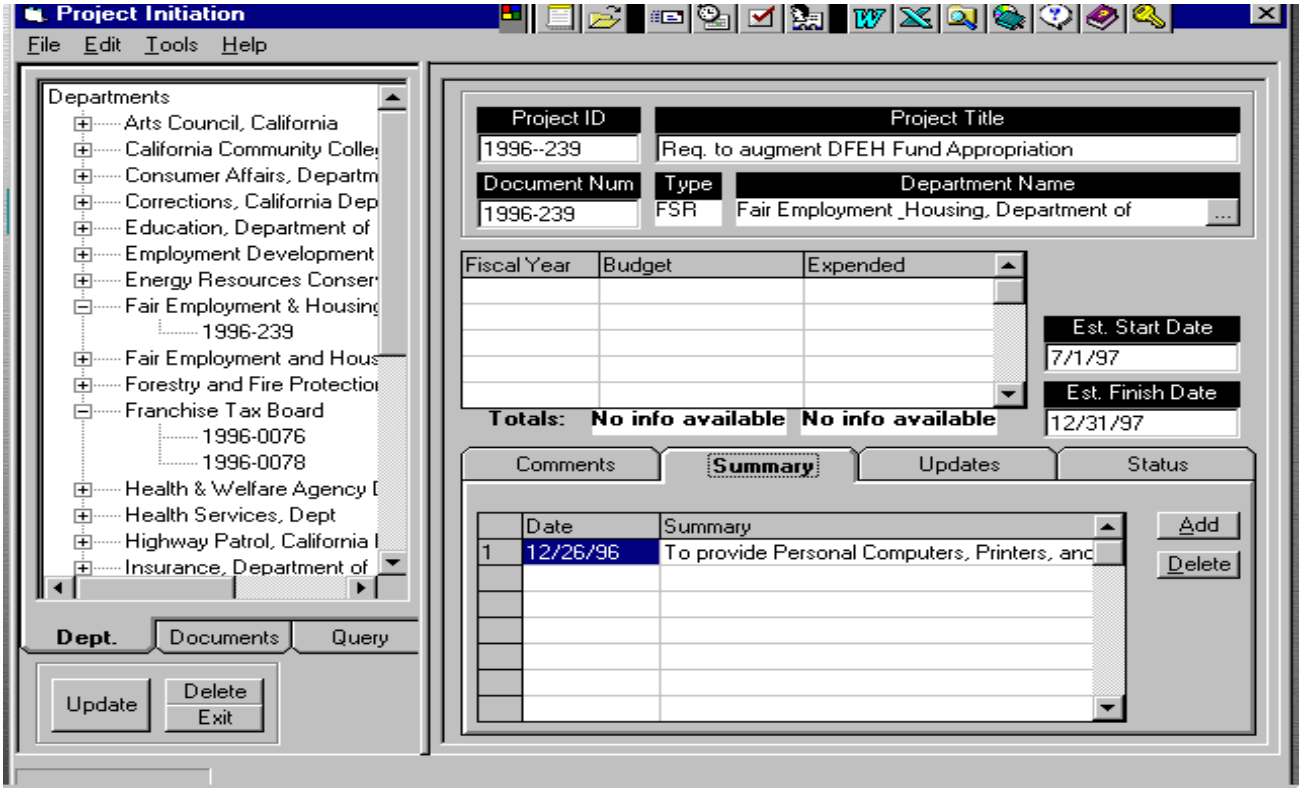
- *Strategic Risk* — The degree to which the proposed project is in alignment with business strategies;
- *Financial Risk* — The probability that the organization will be able to secure funding for the entire project life cycle from sponsoring agencies;
- *Project Management* — The impact on all areas of project management necessary to complete the project, including a realistic time frame, sufficient resources, necessary skill levels and a sound project management approach;
- *Technology Risk* — The degree to which the project must rely on new, untested or outdated technologies, including hardware, software and networks; and
- *Organizational Impact and Operational Risk* — The amount of change needed within the organization as well as the effort required for continued operations at project completion.

These categories form the basis of the DOIT's new RAM. This tool is based on the best features of all the products evaluated and provides a sound model that is uniquely customizable to California's technology programs. It utilizes a standardized questionnaire to assess risk levels, which are produced through an automated report generation feature. The output from this tool, the Risk Assessment Report, provides a thorough overview of project risk areas and can be automatically generated when the survey is completed. The report provides a general summary of risk scores in each of the five risk categories and a detailed analysis of responses to questions.

To ensure that the new tool is accurately evaluating project risk, a small group of projects from the Employment Development Department, Franchise Tax Board, and the Department of Corrections were used as pilots to help calibrate the model. The success of the DOIT's RAM was recognized by the National Association of State Information Resource Executives (NASIRE), which presented the DOIT with the 1997 Outstanding Achievement Award for Administrative Applications.

To ensure that the RAM is accurately evaluating project risk, the DOIT has incorporated numerous suggestions and recommendations from different project managers and released a new version of the RAM in September 1997. The major enhancements included a different risk assessment rating algorithm, an improved questionnaire and screen modifications. By the end of 1998, the DOIT will:

- Use the RAM to assist with the Program Manager Training and Certification program. The RAM will help insure that the project manager with the most appropriate skills, experience and training manages the information technology project.
- Conduct a survey of numerous agencies to substantiate the benefits and identify additional recommendations of the RAM
- Develop a repository of risk assessment scores and risk information for a number of information projects within the state.



On-line Project Tracking Information

One of the greatest obstacles to adequate oversight of IT projects has been the lack of readily available information about the projects themselves. To address this issue, the DOIT developed a data base system that goes far beyond the SB 1 requirement to catalog projects with approved Feasibility Study Reports (FSR). The DOIT has developed the following systems:

- *The Project Initiation and Approval Database (PIP)*, which is accessible to the Legislature and appropriate entities through a secure Internet application, provides an index of proposed projects that have not yet been initiated. This DOIT web site includes an interactive data base of projects with approved FSRs, and will be updated in real-time. PIP contains the project name, description, budget, project manager, program official and other important data.
- *The Project Oversight Tracking System (POP)*, which captures ongoing information about the status, both quantitative and qualitative, of active IT projects. The POP system tracks project schedules, deliverables, risk assessment reports, critical issues and project status. Much of this information comes from independent oversight reports and the departments 'project update and milestone reports.

These data bases do not simply capture projects upon FSR approval; they track the approval process itself, creating a precursor of a "cradle to grave" IT project documentation process. (This documentation process will be an essential tool for creating an inventory of all state IT projects.) The pertinent data was difficult to find, if available at all. From project descriptions and project managers, to budgets, schedules and deliverables, the data that actually existed was

"jailed" in old FSRs, vendor files, project office cabinets, managers' heads and the bowels of disparate accounting systems across the state. This is no longer the case.

Future plans for PIP and POP include direct agency input for projects requiring FSRs and all IT projects, including those instituted through delegated authority or any other means. These data bases will eventually interface with automated project management, scheduling and accounting systems.

Risk Mitigation Program Review

The DOIT has completed an initial evaluation of the effectiveness of the department's initiatives to improve project management over the past 12 months, and the preliminary results are promising. For the first time, there is a centralized, coordinated, structured and effective process to identify, evaluate and monitor IT projects. Certain IT projects will continue to face challenging problems; however, checkpoints are in place to provide an early warning system to afford state IT managers the ability to take appropriate action. These oversight and project management evaluations will be continuous, reflecting the DOIT's total quality management (TQM) approach to the state's investment in IT. The DOIT will be seeking new and innovative solutions to the complexity of managing the State of California's multibillion dollar technology deployment. Most recently, this has involved a DOIT survey via the Internet to identify "best practices" within other states, the federal government, academia and the private sector.

New Contract Procedures

Procurement and implementation of IT projects entail many challenges for the state different from those faced in acquiring traditional goods or services. Unless these challenges are addressed, projects face the risk of missed deadlines, cost overruns, substandard products or even project failure. An example can be seen in the need for contracts specifically geared toward IT projects. In the past, poorly-written contracts failed to provide the state with adequate protection.

The DOIT has worked in conjunction with the DGS to ensure that agencies' and departments' contracts for IT projects contain language which promotes successful project completion with appropriate legal protection. In October, the DOIT issued a Management Memo jointly with the DGS (MM 97-14) establishing contract guidelines for all major IT projects and requiring the use of specific contractual clauses. The policy requirements provide revised language to the state model IT contracts, including:

- A change clause, which provides a definition of certain limited conditions when the state may unilaterally direct a change to a contract;
- A termination for convenience clause, which provides a unilateral right for the state to terminate contracts, in whole or in part, without breach of the contractor;
- A stop work clause, which provides the state a mechanism to halt performance for up to 90 days (or longer if both parties agree) when a problem arises, in order to determine the best course of action to pursue; and
- A disputes clause, which requires internal resolution of disputes and an appeal process before a dispute can be escalated to court action.

The policy also requires additional considerations to address special risks in IT contracts, including:

- Requiring a project plan enumerating specific deliverables or completion of defined tasks and corresponding delivery schedules. All payment schedules should coincide with that plan and be contingent upon the successful execution of those defined deliverables or tasks;

- Requiring creation of an "Executive Committee," a designated group with the authority to resolve potential disputes and approve resulting contract changes in an expedited manner. Executive Committees include representation from, at a minimum, the contractor, agency program management, agency contracting personnel, technical or quality assurance personnel, and those state oversight agencies which have indicated a desire to be included;

- Requiring warranty provisions which provide, among other things, that all work is in accordance with the contract requirements;

- Requiring provisions ensuring that contractor products address Year 2000 solutions; and

- Requiring that the state owns all works of authorship created by or provided by the contractor and related to the project, regardless of form, and whether complete or incomplete.

Phased Implementation

With IT projects, bigger is not always better. The sheer enormity of some IT systems can make them unwieldy, which can ultimately lead to missed deadlines, cost overruns or other project problems. The DOIT is aggressively looking at ways to address this issue in California with alternative approaches to the procurement of state IT services and products. A key policy is the phased implementation of IT projects.

The concept of phased implementation means that a project is divided into distinct and separable tasks, the completion of which enables the department to make use of the deliverables from each particular phase without further work being completed. This approach is specifically intended to enable agencies to minimize risk, maximize value, implement systems quicker, and exercise greater judgment and discretion based on sound management practices.

As an alternative to large comprehensive system development efforts, phased implementation allows projects to be divided into several smaller increments that:

- Are easier to manage individually than one comprehensive approach;

- Address complex IT objectives incrementally to enhance the likelihood of achieving workable solutions for attainment of those objectives;

- Provide for delivery, implementation, and testing of workable systems or solutions in discrete increments, each of which comprises a system or solution that is not dependent on any subsequent increment in order to perform its principle functions; and

- Provide an opportunity for subsequent phases to take full advantage of any evolution in technology or needs that occur during conduct of the earlier increments.

This approach to system development efforts folds in nicely with alternative procurement approaches. The phased implementation contract is an alternative process that provides departments the opportunity to incrementally acquire a system. The phases can be acquired via

a single procurement, or by multiple procurements, but the intent is to ensure that the state is not obligated to purchase more than one phase at a time.

Under the phased implementation approach, the department incrementally awards and manages the project rather than requiring contractors to price and manage the entire effort at one time. This approach allows the agencies to make more informed decisions based on factual information rather than on projections and estimates.

Wherever possible, the initial project phase shall be confined to delivering the essential core functionality that will deliver the greatest portion of the benefits of the proposed system. Features and functions which are not essential to the delivery of core functionality and provide only marginal additional benefit should be planned for subsequent phases. When it is determined that all core functionality cannot be included in a single phase, project phases should be planned so that the majority of high risk tasks, such as applications development and cross-system interfaces, are completed and accepted before high-cost equipment, software licenses, facilities and network expenses are incurred.

Project Management and Project Managers: The Pursuit of Excellence

Project management represents a major category of risk in the implementation of an IT project, and the lack of appropriate project management continues to be a significant deterrent to state efforts to implement projects successfully. Like so much else regarding state IT, it has been up to each individual state department to develop project management expertise. As a result, some departments are better able than others to manage their IT projects; however, even the most experienced department may find its project management capabilities inadequate for a particularly complex project.

As an initial effort to address the disparity among departments regarding project management expertise, the DOIT has, as noted elsewhere in this report, implemented a program to train and certify project managers. Because the program is new, it will not address the immediate need to ensure that state projects are managed by individuals with expertise commensurate with the risk and complexity of the projects to which they are assigned. In the interim, the DOIT will require, as a condition of project approval, that project management be acquired from an external source if insufficient expertise exists within a department. Moreover, a similar requirement may be imposed on currently approved projects in instances where projects exhibit indications of significant problems which can be attributed in part to insufficiently capable project management.

Taking a further step toward generally improving the state's ability to manage IT projects, the DOIT has entered into discussions with representatives of the Institute of Electrical and Electronic Engineers (IEEE) with the objective of establishing a partnership with the IEEE Computer Society to focus on methodologies for improving project management through the adoption and employment of IEEE project management best practices and standards.

The DOIT's approach in this regard will be to work with selected state agencies to act as pilots for the partnership effort. Upon proof of the concept (i.e., an acknowledged improvement in the project management capability of the pilot departments) additional state agencies will be encouraged to adopt the proven best practices and standards. The potential benefits from this approach are substantial, ranging from more successful state projects to significant savings in training, because project managers transferring from one state agency to another will not have to undergo training in a different project management methodology.

Peer Review

The DOIT believes that peer review offers an additional effective mechanism to reduce project risk, from project inception through the implementation cycle. Under this concept, a proposed project would be presented to a panel of peers. The peers could be drawn from within the state, for example through the Information Technology Coordinating Council (ITCC) and also from the California Information Technology Council (CITC).

Peer group presentation and discussion would provide a useful critique to the proposing department, and to ensure that the project is well-grounded. Subsequent periodic peer group sessions throughout the project development cycle would help to keep the project in focus and under appropriate control.

The DOIT anticipates a framework will be in place by early 1998 which will enable a pilot of the concept involving one or more state IT projects.

Project Manager Certification Program

It has been determined that when a California government IT project fails, it is because of a lack of a consistent and uniform approach to the management of state IT projects. For an automation project to be successful through project management efforts, a number of different tools, techniques and strategies must be employed throughout the project life cycle. In particular, automation projects must include:

- ❖ Project management methodology;
- ❖ Structured development methodology;
- ❖ Project management training;
- ❖ Project work plans;
- ❖ Workload estimation;
- ❖ Quality assurance techniques;
- ❖ Contract management; and
- ❖ Project management structure.

By utilizing these various tools and techniques consistently throughout the project life cycle, the state can increase the chances of successfully completing an automation effort — on-time and within budget. Because of the increased dependency on computer systems, the state continues to face increasing pressure to deliver functional and highly usable computer systems in less time.

In 1997, the DOIT took the first step towards addressing the state's project management challenge. The DOIT set policy and guidelines for project manager training and established partnerships with the University of California at Davis (UCD) and the Project Management Institute (PMI) for the training and certification of state project managers.

The objective of the policy and guidelines was to guide and direct departments in the proper matching of project managers to state IT projects based on an assessment of the project's risk. In addition, state and independent certification is required of project managers responsible for medium and high risk projects. The DOIT also developed guidelines and templates that state departments must use in describing project manager's experience, training and certification, and to request policy exemptions.

The DOIT sought a partner to provide training for managers of state IT projects. In April 1997, the DOIT entered into an inter-

agency agreement with the UCD Extension Service to develop such a program. The UCD program entails 220 hours of instruction which, upon successful completion, would give the successful graduate a University Extension, UCD certificate in Project Management.

Candidates have the option of a standard format running approximately 24 months or an accelerated format which can be completed in one year. The DOIT-sponsored UCD program began in June 1997 with courses scheduled every two to three months.

In addition to the UCD partnership, the DOIT also entered into a partnership with the nationally-recognized Project Management Institute (PMI) as an alternative for the certification of state project managers. PMI uses experience, course work and examinations to certify project managers for a vast array of projects — including construction projects, IT projects and massive aerospace projects. In April 1997, the DOIT held a symposium to announce to state departments and agencies that training and certification options were now available through UCD and PMI. Departments began utilizing these options this past summer.

Addressing the Year 2000 Challenge

The Year 2000 dilemma may indeed be California's greatest IT challenge. The Year 2000 represents a threat to computer systems throughout the world. The problem arises because most computer programs created over the last 30 years assume that all dates fall within the 20th century. Unless corrective action is taken, business functions that depend on correct understanding and manipulation of dates will begin to fail as the turn of the century approaches.

California 2000 Project Office

From its inception, the DOIT has recognized the threat of the "Year 2000 problem" to California government programs and the essential services provided to citizens. In response, the DOIT initiated the California 2000 Program and instituted the California 2000 Project Office. The DOIT identified four primary goals of this program:

- Expand executive awareness of the existence and magnitude of the Year 2000 problem;
- Produce a statewide taxonomy of impact, risk and cost;
- Demonstrate leadership, sponsorship and advocacy on behalf of departments and agencies; and

California's Y2K Project Accomplishments

Y2K Issue	Action Taken
■ Project Management	☑ Seminar conducted
■ Vendor Compliance	☑ Surveys conducted
■ Contracts	☑ Language in place
■ Funding	☑ Special funding available
■ Legal	☑ Seminar conducted
■ Staffing	☑ Surveys sent
■ Testing	☑ Seminar planned
■ External Interfaces	☑ Ongoing work with the Y2K Task Force

- Provide guidance and enabling assistance and promote coordination and information sharing to leverage resources and best practices.

Throughout its first full year of operation, the California 2000 Project Office has delivered multiple initiatives to foster California's efforts to successfully meet the Year 2000 needs.

Among the most challenging tasks that the DOIT continues to address is increasing awareness of the existence and magnitude of the Year 2000 problem. Because the problem is relatively easy to understand, many enterprises in the public and private sectors have underestimated the time, effort and cost of fixing the problem. Additionally, it is difficult to interest senior management on a costly IT effort that produces no new or enhanced functions, but simply allows "business as usual" to continue uninterrupted.

The Year 2000 problem has been associated chiefly with computer systems and is widely perceived as a problem to be solved by the IT organization. However, in a world where virtually every business, including government, is dependent on computer systems to deliver basic business functions, failure of the IT systems equates to failure of the business functions.

Over the past year, the DOIT has made a concerted effort to enhance awareness at all levels of state government through presentations to the Governor's office, the Cabinet, the Legislature, directors and department CIOs.

Through these efforts, the Year 2000 problem is increasingly being understood for what it is: a business problem and not an IT problem. In addition to informational presentations, the DOIT has directed the IT organizations it oversees to make their Year 2000 remediation efforts a high priority.

Executive Order

The Year 2000 effort has become a state priority. In October 1997, Governor Wilson signed Executive Order W-163-97, directing all state agencies to correct their Year 2000 problems by the end of 1998. This action by Governor Wilson indicates the seriousness with which the problem is acknowledged at the highest level of state government. Specifically, the Executive Order calls for:

- Limiting new computer projects to those mandated by law;
- Requiring each state agency to take responsibility to find and fix Year 2000 problems by December 31, 1998;
- Protecting essential computer systems from corruption by other systems which are not Year 2000 compliant; and
- Requiring any new purchases of systems, hardware, software or equipment to be Year 2000 compliant.

Governor Wilson's executive sponsorship of this effort now gives the state's IT professionals the commitment they need to follow this mission critical task to completion. The DOIT takes its responsibility for oversight of this project seriously. In response, Governor Wilson gave the DOIT clear performance guidelines to meet, including:

- Defining Year 2000 compliance standards for the state;
- Requiring quarterly update reports from each state agency;
- Providing quarterly Year 2000 progress reports quarterly to the Administration and the Legislature;

- ❖ Fostering solutions to the problems presented by embedded microchips in automated devices; and

- ❖ Addressing Year 2000 legal issues which may directly or indirectly affect state services.

One of the major goals of the California 2000 Program is to develop an understanding of the magnitude of the state's Year 2000 problem and the associated risks and costs. To that end, the DOIT has required every entity it oversees to take an inventory of its IT systems, assess the risk to each of the Year 2000 and determine the appropriate course of remediation.

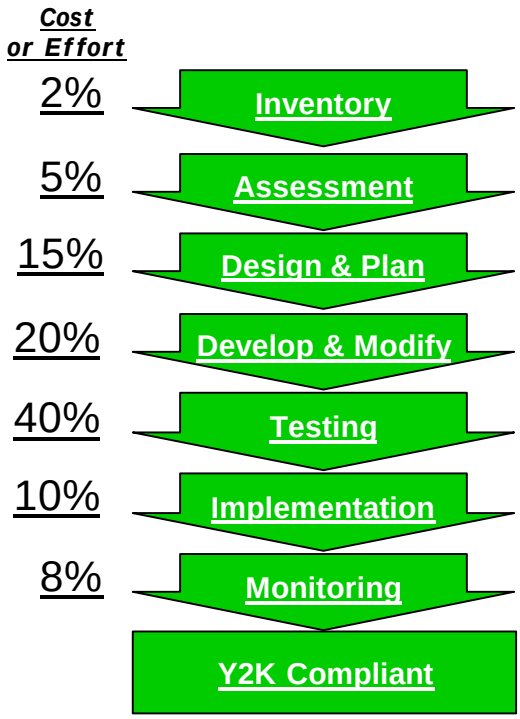
Based on the data supplied by reporting entities, more than 1,200 systems — 600 of them mission critical — require some form of remediation. Current cost estimates approximate $187 million. Remediation of all of these systems will unfold over the course of the remaining years in this century. Unlike other IT projects, Year 2000 remediation projects have a completely inflexible deadline and a predictable consequence if that deadline is missed. As part of its oversight responsibility, the DOIT has instituted a program to oversee century change projects through the Year 2000.

Comparison of planned versus actual effort, schedule and cost is the fundamental principle of project oversight. Because of the inflexibility of the Year 2000 deadlines, the DOIT's oversight process focuses on schedule — on whether or not systems are meeting their planned milestones and implementation dates.

Only four fiscal quarters remain until the end of 1998, and many entities are only now uncovering the magnitude and scope of their Year 2000 challenges. To exercise due diligence, the DOIT must do more than simply track entities'

- **The CA2000 Program requires state entities to provide the DOIT with:**
  - an inventory of all IT systems.
  - an assessment of the Y2K impact on IT systems.
  - a plan detailing activities, overall project costs and schedules.
  - quarterly updates beginning in October 1997.

CA2000 Program Phases



quarterly progress. Therefore, the DOIT requested that entities begin submitting detailed project plans by October 15, 1997. The DOIT is reviewing these plans with the entities and has scheduled face-to-face meetings. For projects deemed to be of significant risk to the state or with a high risk of failure, the DOIT will:

- Require monthly updates to the detailed plans;
- Evaluate progress through analysis of planned versus actual completion dates;
- Conduct monthly project reviews with the Year 2000 project managers and selected project team members; and
- Take appropriate actions, including issue escalation and management intervention, when required.

The 1997/98 Budget Act appropriated $50 million for Year 2000 remediation of the IT systems and directed the DOIT to evaluate requests according to stringent criteria. In order to meet the requirements of the Budget Act and to facilitate funding requests by the state entities, the DOIT developed a comprehensive package for the departments so that requests would have a standardized format and content. The DOIT worked closely with the DOF to ensure that its needs regarding the budget language would be met. The DOIT continues to work with state entities which request Year 2000 funding to ensure the merit of their remediation plans and to validate the funding requests to be processed by the DOF and the Legislature.

Year 2000 Challenge Outreach

The California 2000 Program remains dedicated to providing guidance and facilitating information sharing among state entities. In 1997, the DOIT presented two formal seminars and was heavily involved in Year 2000 seminars presented at the Government Technology Conference (GTC) and the Information Technology Executive Conference.

The Year 2000 presents formidable challenges to project managers. Recognizing these challenges led the DOIT to hold a one-day project management session that focused on project management issues of special significance to Year 2000 project managers. More than 175 state project managers attended this session.

The DOIT also sponsored a seminar on the legal issues related to the Year 2000. More than 50 agency and department counsels and department executives attended this seminar.

The DOIT has continued the communication and guidance efforts it instituted last year, including a Year 2000 web site, the monthly Year 2000 task force meetings and participation in the monthly meetings of the state's Year 2000 project managers.

Over the course of 1997, it has become apparent that the Year 2000 problem is larger and more far reaching than originally anticipated by most of the IT industry. The easily identifiable, and therefore the most likely to be fixed, problems are associated with mainframe systems. The majority of California's IT effort to date has focused in this arena and the state's entities have developed a good grasp of the task ahead of them. Attention must now focus on other areas of technology as well, including desktop, knowledge worker systems, embedded microchip systems and distributed computing.

The DOIT has been charged to initiate a comprehensive analysis of some state IT contracts to identify potential claims and causes of action which may result from the Year 2000 problem. The DOIT has the statutory oversight responsibility and monitoring authority to provide oversight and guidance relating to IT contracts and the Year 2000. As a result, the DOIT is exploring several avenues to anticipate litigation which may involve the State of California as a party plaintiff or defendant.

The Year 2000 Project Office is currently evaluating potential programs to address the risk and impact of the Year 2000 problem to systems containing date-sensitive microchips which are not traditionally managed by the mainstream IT organization. There are few vendors with knowledge and experience in this area of IT.

The risk posed to California by the Year 2000 challenge is not confined to state government. Other public institutions and private enterprises share the same exposures. The DOIT will embark on a program to promote awareness of the Year 2000 problem to California's public and private enterprises beyond the boundaries of state government.

The state's IT systems send and receive data from numerous public and private entities within and outside the state government. Each interchange of data poses a potential threat either that the data itself has been corrupted by a non-compliant system or that it will be misinterpreted by a non-compliant system. The DOIT intends to foster standards to assist state entities in protecting their essential systems from corruption by other systems which are not Year 2000 compliant. On February 19, 1998, the DOIT will co-sponsor with the GTC a summit focusing on data interfaces. Expected attendees include representatives from other states, state departments, counties and municipalities.

The DOIT will employ careful monitoring of planned versus actual schedules and frequent face-to-face project reviews to ensure that the state's Year 2000 efforts are completed on time.

New Trends and Technologies: DOIT's Vision for California's Future

Electronic Government

Few technologies offer as much potential benefit to government and citizens as those associated with the Internet and the World Wide Web. The easy use and low cost of these tools have led to their widespread adoption by businesses, organizations, governments and citizens. The Internet is becoming a universal computer network, used by many businesses and a growing proportion of private citizens, and thus presents a completely new means for government to deliver its services and perform its functions.

In the private sector, these opportunities, and the technical methods of seizing them, are referred to as electronic commerce. These same technologies and applications, with special adaptation to the needs of the public sector, may be thought of collectively as electronic government.

The potential advantages of electronic government are so compelling that there are growing temptations to see it as a panacea for many government problems. Certainly, computers have been essential to the ability of California government to support the population growth of the past two decades without a corresponding increase in the size of government. Many planners believe that the use of computer networks might ultimately lead to a reduction in the size of government while improving the quality of service.

The rapid adoption of the World Wide Web, with its home pages and browsers, has been propelled by the convenience it offers in providing information to a broad, geographically dispersed audience. Information providers can present their messages in clear, accessible and even exciting form, can deliver that information instantly and directly, and can have most of the benefits of a live, interactive exchange without dedicating a lot of personnel to the effort. Information seekers can sort through sources at their own pace, jump rapidly from one subject or provider to another, and do so from the convenience of their home or office at any hour of the day.

California state government has kept pace with this development, with nearly all state agencies offering web pages. Most of those web pages provide substantial information on the functions of their sponsoring agencies, and provide means of contacting the agencies for assistance or services. By July 1998, all such web pages are required by statute to include a complaint form that can either be completed and submitted online, or printed and mailed conventionally. The California State Library has sponsored a particularly high-quality web page that serves as an index and gateway to the individual Internet presentations of the other state agencies. This web page is recognized for its comprehensive and convenient format.

There is substantial public interest in general information, and the electronic delivery of that information at once vastly increases the distribution of that information while reducing the effort involved in responding to public information requests. But the provision of general information, however valuable and important, realizes only a small portion of the potential benefit of electronic government.

The majority of government contact with the public, businesses, organizations and other governments involves either specific information requests or the need to conduct a transaction of some sort. By using electronic government technologies to replace the current methods of these activities, the state can achieve much greater reductions in cost and effort to the state and its clients.

To be sure, there are often significant barriers to these efforts. The private sector has been slow to adopt electronic commerce, despite the obvious potential benefits, because there remain perceived and real immaturities in the necessary technical and business infrastructure.

A basic capability of large shared computer systems is transaction support. Many activities involving entry of information into computer systems are lengthy or complex enough that the activity cannot be completed in one session. The user may be partway through completing a form, for example, and find that all of the necessary information is not at hand. It is more than a convenience, almost a necessity, that the user not have to restart at the beginning when ready to resume.

Similarly, when a session is interrupted, as when a dialup connection is severed, the computer system must be prepared to deal properly with the incomplete activity, either by deleting the partial information or by saving it for later. Yet as fundamental and essential as these capabilities may be, they are only now becoming available in Internet-based electronic commerce products.

There has been considerable discussion of the issues of transmission security and the public fear that transactions they make over the Internet will be maliciously overheard. The structure of the Internet does provide more opportunities for eavesdropping than do telephone networks, but it is fairly easy to encrypt the transmission of sensitive information such as credit card numbers to effectively prevent this.

The ongoing debate of encryption technology strength, while important to international commerce, national security and law enforcement, is largely irrelevant to everyday business and government transactions: bad guys simply are not likely to harness a supercomputer to the task of cracking a code to swipe a credit card number when it is much simpler and less time-consuming to simply rummage trash cans for the same information.

A far more important issue, although perhaps less discussed because it is harder both for the public to understand and for the technical community to solve, is authentication. If the government is going to provide confidential information to a citizen or entity, it is essential that the government be certain that it knows to whom it is sending that information.

Mailed communications depend on the knowledge of an authorized address, and of the ability of the Postal Service to deliver the communication to it. In-person transactions frequently involve matching an identification card to the individual presenting it, usually by comparing photographs, descriptions and signatures. The nature of the Internet makes it impractical to associate an address with an individual, and there is no current method for an individual to present identifying credentials across the network.

Considerable industry effort is being devoted toward this problem and potential technical solutions have been identified. Perhaps most promising is the technology involving digital signatures and certification, with which an individual is assigned a unique digital message, or certificate, that can be transmitted over the Internet to identify that person to a potential business partner, including the government.

This identifier is provided by a third party, known as a certification authority, who presumably initially verifies the person's identity using conventional means, and countersigns that certificate. The government or business does not need to recognize each individual, but needs only to know and trust the certifier's countersignature. Such certificates are used by both parties to a communication: the government agency or business uses a similar identifier, so the individual knows with whom he is transacting business or exchanging secrets.

This methodology provides additional benefits. An individual's certificate includes a unique key, which the government agency or business can use to encode its communications with the individual so that only that individual can read the message, thus preventing problems with eavesdropping or misdelivery. Because only the owner of the certificate knows that key, it can be presumed that only that person can have participated in a conversation using that identifier.

This helps achieve a more difficult task: preventing a person from denying that he or she sent, or received, a particular communication. Known as non-repudiation, this capability is essential for activities, such as tax filings, where the communication, and its accuracy, are enforced by law.

The problem for governments and businesses desiring to employ digital signature technologies is that the technologies are not widely supported by services and products. There are not certification authorities which are performing the initial verification of large numbers of individual identities through in-person interviews.

There are a number of businesses that plan to enter into this field, but they are mostly issuing only business entity certificates or offering "demonstration" certificates to unverified individuals over the Internet.

The certificates themselves are an incomplete product; they consist of hundreds of apparently-random characters, and therefore cannot be memorized. Current implementations involve storing the certificate on a computer, which transmits them as part of secure transactions. Since anyone who has access to the computer has access to the certificate, the computer is authenticated, not the individual.

The solution is probably to store the identifier on a "smart" card, which the owner carries, inserts into a computer, and activates with a memorized password. But at this time, there are few smart cards in circulation, and even fewer computers with suitable smart card readers.

Related to both the problem of secure transmission and authentication is the issue of electronic payment. In the current environment, it is fairly difficult to exchange credit information over the Internet in a safe manner.

As noted earlier, adequate technological solutions have been developed and are available in the marketplace, but there is not yet widespread adoption of those products. Short-term solutions involve performing the financial portion of a transaction "offline"; one can place an order for retail goods or for a government-issued permit across the Internet, but the bill arrives and is paid through terrestrial mail.

In some cases, a pre-transaction exchange of financial information can form the basis for a long and repetitive commercial relationship. The City of Oakland, for example, accepts requests for building permits over the Internet, and bills the contractors using a credit card number they presented in person while setting up their online account.

Within the next year or so, the widespread use of secure Internet browsers will likely allow safe transmission of credit card information to sites the public knows — perhaps by accepting a third-party certificate of authentication from that site — and trusts.

Over the long term, the DOIT anticipates that credit cards and authenticating smart cards are likely to be combined into a single consumer product, so that one is at once authenticated as an individual and as a credit bearer. The DOIT therefore cautions against state efforts to distribute authentication certificates for large portions of the public, as that effort is likely to be superseded by such credit/identity certificates.

Of course, there are simpler ways to achieve many types of safe Internet transactions. Classically, computer network users identify themselves with a user name and associated, memorized secret password. This method is restricted in that it does not itself establish a secure, encrypted conversation, nor will it serve to establish non-repudiation.

Most importantly, this approach is limited in scale: most governments and businesses cannot take on the task of providing user ID/password combinations to millions of citizens, nor will the public tolerate a requirement to remember the user ID/password combinations for dozens of government and business entities.

Nevertheless, this tried and true mechanism will work to support many electronic government applications where the number of transaction partners is relatively small and cooperative, and where non-repudiation is not a significant issue.

Electronic government opportunities can generally be classified into three groups: government-to-government, government-to-businesses/organizations, and government-to-individuals.

They can also be classified into three general types: public, in which positive identification of the transaction parties is not important; private, in which identification is necessary; and official, in which it is necessary to ensure non-repudiation.

The lists are roughly ordered from easiest to hardest to implement in the current environment. By focusing efforts on the easier ends of both groups, the state can develop workable plans to capture immediate benefits from electronic government without accepting unreasonable levels of risk.

Easily the lowest risk activity, and the one most within the span of government's ability to implement, is communication within and between governments. The state can gain valuable technical experience, and can obtain modest but worthwhile benefits, simply by using electronic means to conduct internal business between departments.

Many of the transactions between the state and local governments have already been converted to electronic means, and others are underway, but many opportunities remain to reduce paper workflow costs and improve information accuracy and timeliness. Even the most cautious government entities should be willing to explore these possibilities.

Almost as safe are potential government-to-business electronic links. It is easy to establish even the most secure communications relationships with individual business partners and with the relatively small groups of businesses involved in most government activities.

For example, the DOIT has established fully secured, authenticated connections between agency information security officers and the contract service provider for reporting and obtaining assistance for computer security incidents.

While industry has been as slow to implement electronic commerce as has government, there should be a shared interest in both the cost and time reductions available through electronic transmission of transactions and in developing this capability in a controlled environment.

A solid first step is for government to include electronic commerce provisions in the business specifications for new systems involving government-to-business communications. These should include not just the ordering of goods, as will be implemented with the new online procurement system currently planned by the DGS, but the transmission of all repetitive communications and transactions involved in any ongoing government-business relationship.

Even greater benefits can be derived from adding electronic communications to the larger state government-to-business processes, such as licensing and regulation, financial filing and information retrieval. Many of these systems are already automated, and while in some cases the existing automated systems are neither amenable to electronic commerce nor easy to change, in other cases these existing systems can serve as an enabling foundation.

There are broad classes of government-to-public transactions that can be safely delivered through the Internet and related mechanisms. Many types of actions involving permits and fees do not require establishment of identity. These can be requested by the public over the Internet, and either mail-invoiced and then delivered when paid, or transacted by credit card exchange from persons with secure browser capability.

Even when a transaction involves a certain degree of identification, as for fishing licenses which require demonstration of residence to obtain a lower fee, other states have established mechanisms to lookup and compare driver's license numbers with name and address information stored in motor vehicle files.

In many of these cases, improved ease of access is likely to increase revenues both by making compliance convenient and expanding geographic reach to out-of-state locations.

Many government and technology leaders who recognize the potential benefits of electronic commerce and electronic government are frustrated at the slow pace at which business and industry are adopting such systems. These visionaries and technology entrepreneurs see the technology as ready and wonder what's keeping everyone. Much of the problem, of course, is simply the difficulty of making such a dramatic change in a commerce system that in some regard has changed little in many centuries. As already discussed, there are many areas in which the technology is quite ready to perform.

There are other areas that are simply not ready. The state should not plan to implement any transaction where it may be necessary to prove that an individual performed a particular transaction unless the number of potential business partners is small enough to allow the state to individually assign user IDs and passwords or other authentication.

Other activities, such as election balloting, are simply too prone to fraud and the consequences of malfeasance too great for existing technology to reliably address. There are many technologists who believe that even the few businesses which are conducting retail business over the Internet are exposing their customers, and stockholders, to serious risk. If so, those businesses may pay the price through the loss of customers, lawsuits or bankruptcy.

The state can not accept such risks; even a minor embarrassment may delay the ability to obtain the benefits of electronic government for years. A major mistake with elections, taxation, licensing or law enforcement could have serious consequences.

In many cases, the very scale of the problem is daunting. There are more than 30 million Californians and huge numbers of homes, vehicles, drivers, businesses and computer users. Even a tiny fraction of such users would overwhelm most existing computer systems, which are designed for only a few hundred users.

Giving access to many government computer systems by adding an Internet connection would lead only to disrupting the government's use of those systems while frustrating those attempting Internet access.

The state's provision of election results over the Internet in November 1996, while a triumph of public information and technical achievement, flooded and nearly sank the entire Internet infrastructure in Northern California. Careful planning, and an expectation of substantial costs, should accompany any effort to hook the Internet up to the state's existing computer systems. At this point, it is also important to note that the cusp of the electronic commerce revolution coincides with the end of the century. Many, if not most, of the world's computer technologists already have their hands full dealing with Year 2000 problems.

More subtle, but equally inhibiting, is the fundamental problem of networking. Instead of building a system, networking involves building relationships between systems. Agreement on everything from wiring to the format of street addresses, and everything in between, must be negotiated, agreed upon and often translated to complete a single functional connection.

Establishing this sort of communication between branches of the same government is often excruciatingly difficult and slow. Building connections between government and millions of individuals is unlikely to prove much easier.

Again, electronic commerce represents an historic change in one of the fundamental components of civilization and government. Haste is neither wise nor possible, but careful and considered implementation of these technologies, with sensible plans, persistent leadership, and real partnerships with industry, can truly achieve better, faster, cheaper and friendlier government.

The Internet and State Government

Public Access

The prevalence of the Internet in state government allows new opportunities to provide more information to the public, but the increased technology creates new challenges as well. Many of these new opportunities and challenges are being addressed in a legislatively required report by the DOIT "outlining a method whereby the public may access by remote access only non-confidential public records, indexes, and data bases contained on state networks."

While public access questions are traditionally concerned primarily with material that is defined as a public record according to the California Public Records Act (Government Code section 6250, et. seq.), the DOIT report considers that issue in the broader context of the electronic delivery of government information to the public. The report makes several specific recommendations for the electronic dissemination of public information, and includes some cautions regarding limitations in the ability of the state to rapidly achieve an environment in which all public records are available electronically.

The state is currently required to make public records available on request. In many cases, there are benefits in convenience and usability in that provision that could be obtained if that information were available electronically. At first glance, it may appear that it would be a simple task for the state to provide electronic versions of information that the state already maintains in that form. But there are significant associated technical, fiscal and public policy issues, especially on a broad scale. These issues, and potential means to address them, are largely common to a larger effort for electronic delivery of government services.

It is particularly important to note that the electronic form in which state government stores records is usually very specific to the state's

functions. In addition, the majority of the state's computer systems are mainframe-based, and not particularly compatible with personal computer environments. Even the concept of a "record" in these systems is often quite different than what is meant by or is usable as a "public record."

The report examines both this internal state technical environment, and that of the public that would benefit from electronic delivery of information. Of particular concern is the issue of privacy. For example, it may be possible to combine multiple sources of public information to accurately infer much less public — and even confidential — information about individuals when those sources are readily accessible by computers.

The report concludes that the electronic provision of public records is generally achievable only with the use of computer systems designed and implemented to support this capability. The report further suggests that the state's efforts to provide information to the public in electronic form would reach the largest possible audience, and could be provided most conveniently and efficiently through use of the Internet and associated vehicles such as the World Wide Web and browser technology. The report therefore recommends that general efforts towards the distribution of public information be through this vehicle.

The report further recommends that all new computer systems be designed to support Internet access to public information that will be created, stored or transmitted by such systems. The report recommends that existing information sources be either converted or adapted to support public access only when the utility of that information justifies the effort that would be required. The report also recommends that the California State Library, through the California Home Page, be supported in its current efforts to ensure that state information provided through the Internet is presented and organized in a manner that facilitates public use and easy access.

Finally, the report notes that earlier experiences with public access to government information, and more recent efforts with the Internet, suggest that the value of read-only access to information is of relatively little utility to the majority of the public. Instead, the public is better served when information is presented along with the means to update, correct it or to otherwise conduct business with the government. The potentially great difficulty of providing public records electronically suggests that any such efforts be undertaken with a consideration for the associated electronic government services that would maximize the value of such efforts.

Statewide Internet Usage Policy

The astounding growth of the Internet illustrates the many benefits technology can offer to government. All state agencies have recognized the Internet to be an invaluable research and communication tool, and most have used it to publish their mission, function, structure, information required by law or other material of general interest to the public. However, as Internet usage by its employees increases, so too does the state's risk of problems and abuse: "surfing" the Internet for purposes other than state business may reduce office productivity; state networks could be jeopardized by viruses downloaded onto the system; inappropriate use of the Internet by employees on state time could subject the state to liability.

Due to the newness of the technology, the state previously had little guidance to distinguish between acceptable and inappropriate Internet activities. To provide direction to state agencies and departments, the DOIT issued a Management Memo (MM 97-03) in January 1997 establishing a Statewide Internet Usage Policy. The Management Memo, which requires agencies and departments to create and implement internal policies, provides a framework for appropriate Internet usage. Some of the issues addressed by the Statewide Internet Usage Policy include:

- Establishing that the state reserves the right to monitor and/or log all network activity with or without notice, including e-mail and all web site communications, and therefore, users should have no reasonable expectation of privacy in the use of these resources;

- Uses that are acceptable and encouraged, such as communications and information exchanges directly relating to the mission, charter and work tasks of the agency, announcements of state laws, procedures, hearings, policies, services, or activities, for advisory, standards, research, analysis, and professional society or development activities related to the user's state governmental duties, and in applying for or administering grants or contracts for state government research programs;

- Uses that are unacceptable, including material which violates or infringes on the rights of any other person, contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal information, or usage which violates agency or departmental regulations prohibiting sexual harassment, restricts the efficiency of the computer systems, or uses the system for any other illegal purpose;

- Existence of copyright laws and the consequences of copyrighted material;

- The proper use and risks of downloading public domain programs;

- The proper use of electronic mail, including a statement that e-mail is considered network activity, and as such, is subject to all usage policies;

- The responsibilities and procedures for regulation and enforcement of the policies; and

- Limitations of governmental liability.

The Management Memo also provides guidelines to agencies and departments for developing their Internet policy as part of their overall IT strategy. These guidelines cover such topics as: Internet planning, access, connection and software; agency home pages; Internet security; computer ethics and etiquette; and computer law and computer crime.

Most agencies and departments have implemented or are in the process of developing their internal Internet usage policies. The DOIT has made itself available to all agencies and departments regarding any direction or assistance in the drafting or implementation of their policies.

Statewide Messaging

Electronic mail is no longer just a powerful tool for communications within organizations. The development of the Internet as a universal network has been accompanied by the rapid adoption of Internet-compatible mail systems. Government planners need to begin thinking of electronic mail – or e-mail – as a means for communicating with the public, businesses, organizations and other governments, and to adopt e-mail strategies that enable such communications. E-mail is thus one of the family of related tools, systems and technologies that will help the state transform the way it conducts the business of government to create easier, more convenient, more comprehensive, and yet less expensive means of delivering its services.

The 1996 DOIT Annual Report described four major goals for the state's electronic messaging systems. The past year has seen both state and industry progress towards each goal, although both the available products, and the state's implementation of them, remain immature. Nevertheless, it now appears probable that the state will be able to define, and ultimately achieve, a course toward the achievement of all of these goals, and to do so in a manner that is consistent with the overall strategy to develop a network of message systems that support electronic government. These goals include:

- Increase the abilities to exchange complex material in addition to brief text messages;
- Improve the ability to readily locate the e-mail address of proposed correspondence partners;
- Enhance the overall security of e-mail to prevent eavesdropping and other abuses; and
- Reduce the difficulty and cost of maintaining e-mail systems.

The adoption of a single vendor product would increase the ability to achieve each of these goals, especially with the current level of product evolution, but such standardization is neither consistent with state policies for open procurement, nor attainable without considerable expense.

More importantly, the overall strategies for electronic government and broader interoperability with the environment outside of government will require the use and implementation of products and processes that will ultimately render single-product standardization unnecessary.

The ability of e-mail systems to exchange more than simple messages depends both on the capabilities of the e-mail systems themselves and on the computer systems that are used to create and view the other material.

Many e-mail systems have for some time had a rudimentary capability, known as UUENCODE/UUDECODE, for attaching non-text material to messages. While this capability is crude and somewhat unreliable, the greater barrier to attachment exchange generally has involved the incompatibility of the word-processing, spreadsheets, geographic information systems, video players and related tools specific to the material. In some areas, such as video and sound, standardization of material and products is fairly common. In others, such as word-processing and spreadsheets, there remains considerable incompatibility in the formats used by different products, which seem to prefer inclusion of conversion routines for "foreign" material, and to revise their own formats with each release to complicate interoperability even with earlier versions of the same product.

For e-mail itself, the ability to exchange documents is improving as UUENCODE/UUDECODE is replaced by the much more robust MIME protocol, and its more-secure enhancement S/MIME.

Within state government, the ability to exchange complex material has improved considerably in the past year as e-mail systems with document interchange capabilities are more widely implemented, and as the proliferation of word-processing and spreadsheet products has decreased with the growing dominance of a few vendor office products.

Even so, the overall situation in state government still remains somewhat frustrating for users who want to exchange material outside their organizations, because the rapid rate of change in

proprietary vendor products continues to result in both governments and their business partners using a broad variety of incompatible products.

As in many other areas, the Internet is providing the strongest impetus towards interoperability in word-processing and publishing.

The ability to locate the e-mail address of a desired destination has shown the most encouraging progress during the past year.

While many vendors are persisting in their efforts to differentiate their products from the competition, often at the expense of interoperability, the demands of the Internet and customers are forcing some real progress.

In particular, it is becoming more clear that the adoption of the standard LDAP protocol for exchanging e-mail directory information between dissimilar systems will soon result in the ability of a user to obtain real-time access to addresses contained in directories outside the user's organization. Each local e-mail system maintains its own directory addresses for its own users. The current mechanism for locating addresses outside this environment is to periodically copy, and perhaps translate, the external directories into the directory of the local system.

This mechanism is inherently unsatisfactory, for it is only as current, and accurate, as the last update, and is limited in scalability to the number of separate translations the e-mail administrator can maintain and the total number of addresses each system can contain. A better approach involves the dynamic, real-time reference to the directories maintained in other systems when an address is needed. This capability, based upon LDAP version 3, is at once current, does not require the copying or translation of directories, and is included in the announced product plans for most major e-mail systems.

The Teale Data Center has established a central mail directory of state personnel, accessible through the Teale web page, which allows anyone to search for a name and to obtain the e-mail address for that person.

Teale plans to use this directory, which currently depends upon laborious copying and translation of the many state e-mail directories, as a basis for a central reference directory which will allow compatible e-mail systems to find and directly read e-mail directory entries throughout state government. This capability will depend upon the delivery of suitable vendor products, and will begin to be available during the next year.

Security in e-mail systems similarly depends upon the capabilities included in products and on the compatibility of those capabilities in the products at both ends of a communication. Encryption of both messages and attachments is now possible with current product implementations, but generally only when the sender and receiver use identical products.

Moreover, encryption remains an option, selected on a per-message basis, to avoid the significant processor workloads and consequent transmission delays required for a secure exchange. State departments vary in their rates in adopting secure-enabled e-mail products, and their implementation of procedures and policies for secure e-mail exchange. As for other e-mail capabilities, current achievement is quite limited, but the prospect for considerable progress in the next year is promising.

The cost and difficulty of maintaining e-mail systems is large and of growing concern to both product developers and system owners. Although this issue is common to the office and desktop automation environment in general, e-mail has been notable for the relatively great difficulty of system administration, especially when compared to the somewhat intangible benefits of e-mail

system use. New vendor products have clearly been designed to address this concern, and are beginning to provide significant improvements.

Certainly, the advances in directory interoperability will offer a direct benefit to system administrators as well as users. Much of the effort by vendors who provide e-mail as a part of a broader office automation and networking strategy has been to integrate e-mail directories with the other tables of user attributes and capabilities, including file and resource access permissions, customization preferences and security profiles.

This integration may ultimately result in a substantial gain in convenience to users, especially those who work from more than one location, as well as to the personnel who must maintain these user definitions. Newer e-mail products are also designed to reduce the effort involved in routine file maintenance, system recovery and similar tasks. Again, state progress toward these goals is largely constrained by the rate at which better vendor products become available and the ability of state agencies to acquire and implement the new products. A related effort involves the exchange of technical knowledge and experience between state agency personnel. Recent efforts sponsored by the DOIT and the consolidated data centers to develop working groups of e-mail and office automation system administrators will provide benefits both in skill transfer and in managing vendor priorities and services levels. But while such efforts are valuable and productive, cost-of-ownership improvements are even more likely than other areas to continue incrementally over an extended period as e-mail matures both functionally and administratively.

With the exception of cost-of-ownership issues, the remaining functional goals for state e-mail systems depend as much on the progress external to individual government agencies as inside. The exchange of message attachments, security in communication, and easy-to-find directory entries all depend on the capabilities of both correspondents.

While state government could make dramatic progress towards these goals by adopting a single product, this effort would ultimately produce only a marginal benefit. The overwhelming majority of state e-mail traffic, like other forms of communications, occurs either within an individual department, or between the department and persons and entities outside of state government. Relatively few persons in most departments communicate with those in other state departments, and this traffic is usually related to control and service agencies such as the DOIT, the DOF, the DGS, and the central data centers. The real benefits from e-mail improvements will derive from enhancements in the ability to communicate with non-state entities, and this will require that the state maintain a strict adherence to Internet-based interoperability. This is, of course, the same strategy as is necessary to enable the state to evolve towards electronic government.